МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
другого магістерського рівня вищої освіти
на тему:

АВТОМАТИЗАЦІЯ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

СТУДЕНТ: Андрущенко Катерина Юріївна _____
(підпис)

КЕРІВНИК: д.е.н., проф. Легомінова Світлана Володимирівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2022

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Спеціальність 125 Кібербезпека

Спеціалізація Управління інформаційною безпекою

Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 2022 р.

ЗАВДАННЯ

на кваліфікаційну роботу

студенту Андрущенко Катерині Юріївні

Тема роботи «**АВТОМАТИЗАЦІЯ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ**», затверджена наказом по університету № 122 від «12» жовтня 2022 р.

1. **Термін здачі** студентом оформленої роботи «22» грудня 2022 р.

2. **Об'єкт дослідження:** автоматизація процесу реагування на інциденти інформаційної безпеки організації.

3. **Предмет дослідження:** особливості побудови автоматизовананих сценаріїв реагування на інциденти інформаційної безпеки організації.

4. **Мета дослідження:** розробка сценаріїв реагування на інциденти інформаційної безпеки організації.

5. **Перелік питань, які мають бути розроблені:**

5.1 Дослідити теоретичні аспекти побудови ефективного автоматизованого процесу реагування на інциденти інформаційної безпеки організації

5.2 Проаналізувати методи та інструменти для побудови автоматизованих сценаріїв реагування на інциденти інформаційної безпеки організації

5.3 Розробити та запропонувати сценарії реагування на інциденти інформаційної безпеки організації

6. **Дата видачі завдання «**«19» вересня 2022 р.

Науковий керівник	_____	С.В. Легомінова
	підпис	
Завдання прийнято до виконання	_____	К.Ю. Андрущенко
	підпис	

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

студенткою Андрущенко Катериною Юріївною

Дата видачі завдання: «19» вересня 2022 р.

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2022	
2.	Збір та аналіз літератури.	03.10.2022	
3.	Написання розділу 1.	17.10.2022	
4.	Написання розділу 2.	31.10.2022	
5.	Написання розділу 3.	14.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2022	
7.	Оформлення роботи	08.12.2022	
8.	Оформлення презентації	15.12.2022	
9.	Отримання рецензії на роботу.	23.12.2022	
10.	Захист в ДЕК	17.01.2023	

Студент _____ К.Ю. Андрущенко

(підпис)

Науковий керівник _____ С.В. Легомінова

(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці прикладів автоматизованих сценаріїв реагування на інциденти інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 5 рисунків, висновків та списку використаних джерел, що містить 20 найменувань. Загальний обсяг роботи становить 78 аркушів, з яких 3 аркуша займає список використаних джерел.

Об’єкт дослідження – автоматизація процесу реагування на інциденти інформаційної безпеки організації.

Предмет дослідження – особливості побудови автоматизованих сценаріїв реагування на інциденти інформаційної безпеки організації.

Мета роботи – розробка сценаріїв реагування на інциденти інформаційної безпеки організації.

Для досягнення кінцевої мети в роботі розглянуто типові проблеми, з якими стикається організація при побудові процесу реагування на інциденти інформаційної безпеки, наведено загальні рекомендації для ефективного реагування на інциденти, а також розглянуто міжнародні стандарти інформаційної безпеки з рекомендаціями щодо побудови ефективного процесу реагування на інциденти інформаційної безпеки. Для наведення прикладу процесу розробки сценаріїв реагування визначено загальні можливості тестової організації і на основі наявних інструментів інформаційної безпеки послідовно побудовано приклади сценаріїв реагування на інциденти типу і «Фішинг» і «Зловмисне програмне забезпечення».

Галузь використання. Розроблені сценарії реагування, а також принцип правильної послідовності розробки сценаріїв реагування можуть бути використані будь-якою організацією в якості прикладу при побудові власної системи реагування на інциденти. Найбільш доцільним використання наведеної методики буле для великих організацій, що мають на меті впровадити або виправити вже існуючу систему реагування на інциденти інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ, ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СЦЕНАРІЇ РЕАГУВАННЯ, АВТОМАТИЗАЦІЯ, ПОШИРЕНІ СТАНДАРТИ.

ЗМІСТ

ВСТУП

А к т у а л ь н і с т ь т е м и. На сьогоднішній день ландшафт кіберзагроз змінюється настільки швидко, що командам безпеки складно організувати швидкий і ефективний процес реагування. Щодня аналітики приймають рішення, які можуть вплинути на всю організацію і безпека організації надмірно залежить від персоналу, який часто використовує ручні процеси для обробки сповіщень безпеки і величезної кількості даних з різних систем захисту інформації.

Неправильно обраний процес реагування, відсутність доступу до необхідних систем, перенасиченість даними з різних рішень, виконання постійно повторюваних дій – все це ускладнює процес реагування і становить загрозу для організації.

Одним із завдань менеджерів інформаційної безпеки організації є побудова ефективного процесу реагування на інциденти інформаційної безпеки.

Розробка ефективних сценаріїв реагування потребує високого рівня кваліфікації відповідального співробітника. В мережі достатньо багато інформації по організації процесу реагування на інциденти інформаційної безпеки, проте доволі складно знайти коректно розписаний підхід до побудови сценаріїв реагування, які є обов’язковими для забезпечення автоматизації реагування на інциденти.

Проведене дослідження може слугувати основою і прикладом для побудови автоматизованих сценаріїв реагування на інциденти інформаційної безпеки в організації.

М е т а і з а в д а н н я д о с л і д ж е н н я. **Мета роботи** полягає в розробці сценаріїв реагування на інциденти інформаційної безпеки організації.

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Дослідити теоретичні аспекти побудови ефективного процесу реагування на інциденти інформаційної безпеки.

2. Описати принцип розроблення сценаріїв реагування на інциденти інформаційної безпеки.

3. Описати тестове середовище, параметри якого будуть використані про розробці прикладів сценаріїв реагування.

4. Розробити приклади сценаріїв реагування для декількох актуальних типів інцидентів з демонстрацією використання наведеного принципу.

Об'єкт дослідження – автоматизація процесу реагування на інциденти інформаційної безпеки організації. **Предмет дослідження** – особливості побудови автоматизованих сценаріїв реагування на інциденти інформаційної безпеки організації.

Наукова новизна одержаних результатів. Розроблені сценарії реагування на інциденти обраних типів можуть бути використанні при плануванні процесу реагування на інциденти інформаційної безпеки в організації. За наведеним принципом можна спланувати процес реагування для інциденту будь-якого типу. Зважаючи на недостатність або відсутність подібних матеріалів у загальному доступі, а саме ключових моментів розробки автоматизованих сценаріїв реагування, наведений в роботі підхід систематизує інформацію по розробці сценаріїв реагування на інциденти і забезпечує організацію чіткою послідовністю дій планування і розробки.

Практичне значення одержаних результатів. Розроблені та запропоновані автором сценарії і наведений принцип побудови плейбуків для систематизації і автоматизації реагування на інциденти можуть бути використані будь-якою організацією, що має на меті побудову ефективного процесу реагування на інциденти інформаційної безпеки.

Розділ 1

ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ЕФЕКТИВНОГО АВТОМАТИЗОВАНОГО ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1. Проблематика процесу реагування на інциденти інформаційної безпеки організації

1.1.1. Роль розслідування інцидентів в побудові системи інформаційної безпеки організації

На сьогоднішній день інформація відіграє надзвичайно важливу роль. Володіння певною інформацією означає володіння певною цінністю суспільного характеру. З нею тісно пов'язані численні права і свободи громадян, життєві інтереси суспільства та держави [1].

У сучасному світі інформаційних технологій проблема інформаційної безпеки набула особливого значення. Сьогодні інформація, що зберігається і обробляється в кіберпросторі та гіпотетично може відбутися її виток до інших осіб, може призвести до технологічних аварій, військових та політичних конфліктів, дезорганізації державного управління, проблем у енергетичній сфері, фінансової системі. У зв’язку із все зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і пильної уваги.

Нині перед суб’єктами підприємницької діяльності гостро стоїть питання щодо вирішення спільної проблеми — інформаційної безпеки організацій та підприємств та незалежно від їх форм власності.

Тільки наявність достатніх сил та засобів охорони інформації може гарантувати успіхи в економічній сфері не лише одного окремо взятого підприємства чи організації, а й в масштабах держави [2].

Забезпечення інформаційної безпеки організації включає в себе велику кількість чинників. Одним із важливих моментів організації захисту інформації є використання комплексного підходу до побудови системи інформаційної безпеки.

Основною метою створення системи інформаційної безпеки організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів інформаційної безпеки. Процес управління інцидентами інформаційної безпеки – ключовий процес у системі інформаційної безпеки. Він включений до рекомендацій ITIL (Information Technology Infrastructure Library) і стандарту ISO/IEC 27002.

Реагування на виникаючі надзвичайні ситуації, пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди [4].

Найбільш складним питанням в процесі управління інцидентами інформаційної безпеки є розслідування інцидентів безпеки. Але часто розслідуванню інцидентів в організаціях приділяють недостатню увагу. Як тільки наслідки інциденту усунені та бізнес-процеси відновлені, подальші дії щодо розслідування інциденту і здійснення коригуючих і превентивних заходів часто не виконуються [3].

1.1.2. Типові проблеми організації команди реагування на інциденти і їх вирішення

У непередбачуваному протистоянні кібер-зловмисникам добре підготовлені групи реагування на інциденти є потужною зброєю в арсеналі організації. Відповідаючи за оцінку систем безпеки та реагування на загрози інформаційній безпеці організації, групи реагування на інциденти відіграють

важливу роль у вирішенні проблем і контролі збитків у системі, виявленні зловмисного програмного забезпечення та інших подіях безпеки [5].

Втім при побудові системи реагування на інциденти інформаційної безпеки необхідно враховувати типові проблеми, що можуть завадити ефективності процесу реагування і знецінені всі вкладені ресурси. Найбільш поширені проблеми включають [5]:

1) Плани не пристосовані до організації.

Проблема: багато організацій впроваджують типові плани реагування на інциденти, в яких детально перераховуються всі кроки, які слід зробити для розслідування потенційного інциденту. Хоча це може здатися правильним ретельним підходом, це часто може надто ускладнити процедури реагування та уповільнити розслідування. Готові плани часто застаріли та неефективні проти нових загроз і мінливих технологій.

Вирішення: організаціям слід впроваджувати політику, процеси та процедури, які адаптовані до їх умов, середовища, персоналу реагування та, що найважливіше, бізнес-цілей. Документація має бути стислою та постійно вдосконалюватися, щоб відповідати як вимогам нормативних документів, так і змінам бізнес-цілей.

2) Плани випробовуються лише в реальних інцидентах.

Проблема: при побудові інформаційної безпеки організації планування базується лише на теоретичному розумінні. Організації створюють комплексні плани реагування на інциденти, але іноді не перевіряють їх, доки не станеться реальна подія. І тільки при виникненні реального інциденту виявляється, що план є провальним з першого кроку. Крім того, багато організацій розглядають створення плану реагування на інциденти як одноразову подію, а не як постійний процес. Як наслідок, плани містять неправильну інформацію щодо інструментів і людей або детальні кроки, які не працюють або не відповідають вимогам.

Вирішення: Організації мають регулярно перевіряти свої плани реагування до того, як станеться справжній інцидент. Відсутність плану

реагування на інцидент може призвести до збільшення часу реагування, плутанини та, що найгірше, переривання бізнес-процесів.

3) Між відділом реагування і співробітниками інших команд виникає дискомунікація.

Проблема: оскільки в більшості організацій безпека інформаційних технологій характеризуються сегментованими функціями, такими як сканування вразливостей, їх виправлення та адміністрування систем, пошук та залучення ключових співробітників інших відділів може бути серйозною проблемою.

Вирішення: централізована інформаційна панель, де група реагування на інциденти може публікувати подробиці про поточне розслідування та отримувати необхідну інформацію, може допомогти вирішити складність в постійному обміні повідомленнями електронної пошти, які можуть перевантажувати скриньки електронної пошти та призводити до пропущених повідомлень або суперечливої інформації. Крім того, цю систему інформаційної панелі можна налаштувати для обмеження доступу або додавання людей за потреби без надсилання дублюючих електронних листів.

4) Командам не вистачає навичок, вони неправильного розміру або погано керовані.

Проблема: усі організації, незалежно від розміру, стикаються з проблемами, коли справа доходить до вибору правильного персоналу для укомплектування групи реагування на інциденти. Маючи обмежені бюджети безпеки, невеликі організації можуть покладати обов’язки з реагування на інциденти на системних і мережевих адміністраторів, які володіють технічними знаннями та історичним розумінням того, як працюють системи, але не мають досвіду прийняття рішень, що впливають на бізнес під час кризи чи порушення. З іншого боку, великі організації намагаються розподілити найбільш ефективну кількість ресурсів для групи реагування на інциденти, припускаючи, що більше персоналу означає більші можливості.

Вирішення: організації повинні уважно оцінити потребу в додатковому навчанні або внутрішній допомозі з найму персоналу, щоб сприяти розвитку належного рівня досвіду в групі реагування на інциденти. Крім того, сильні лідери, які керують командою, повинні чітко визначати ролі та обов'язки, сприяти тіснішій співпраці та покращувати комунікацію з командою та за її межами.

5) Діяльність служби підтримки може знищити важливі докази.

Проблема: про проблеми з комп'ютером, які можуть свідчити про зараження шкідливим кодом, часто спочатку повідомляють у службу підтримки. Якщо співробітники служби підтримки погано знають потреби служб реагування на інциденти, їхня робота з вирішення проблем користувачів може знищити ключові докази. Наприклад, інсталяція програмного забезпечення, запуск антивірусних засобів або інструментів очищення, налаштування параметрів системи можуть перезаписати інформацію, яка може бути безцінною для служб реагування на інциденти. Поєднати ланцюжок подій може бути неможливо, особливо якщо початкові дії не були задокументовані. Агентства, які використовують субпідрядників як службу підтримки IT, повинні переконатися, що співробітники служби підтримки знають про ситуації, які потребують участі групи реагування на інциденти.

Вирішення: якщо співробітники служби підтримки підозрюють, що проблема користувача може бути спричинена зловмисним кодом, вони повинні створити образ пам'яті системи, перш ніж вносити будь-які інші зміни. Довідкову службу також слід навчити документувати свою діяльність у випадку, якщо її дії стануть частиною розслідування.

6) Інструменти реагування на інциденти некеровані, не перевірені або недостатньо використовуються.

Проблема: організації можуть спостерігати неочікувані затримки в процесах розслідування інцидентів і їх усунення, якщо групи інструментів покладаються на пошук інформації про уражені системи, а люди неправильно їх використовують. Навіть найновіші та найкращі технологічні рішення можуть

не забезпечити послідовний, надійний результат без належного планування, інвестицій та обслуговування.

Вирішення: організації повинні підтримувати інвентаризацію інструментів централізовано та слідкувати за своєчасним оновленням ліцензії і оновленням функціональних компонентів. Крім того, членів команди слід постійно навчати всьому набору інструментів. А також інструменти слід регулярно оцінювати, щоб визначити, чи можуть вони протистояти найсучаснішим загрозам.

7) Дані, що стосуються інциденту, недоступні.

Проблема: коли інформація, що містить відповідні деталі атаки, не існує або не є легкодоступною, виникає каскадний ефект протягом усього процесу реагування на інцидент. Зрештою, групі реагування на інциденти важко оцінити вплив, мінімізувати збитки та повідомити про це керівництво.

Вирішення: щоб вирішити цю проблему, організації повинні розуміти, які джерела даних вони мають, які дані вони збирають та як вони керують своїми даними. Залучення власників технологій та оцінка системи управління активами є хорошими способами розкрити весь діапазон потенційних джерел даних. Крім того, група реагування на інциденти повинна ідентифікувати сигнальні події (наприклад, невдала автентифікація, видалення журналів, інтерактивний вхід тощо), які можуть надати контекстну інформацію про інцидент, і встановити процеси для агрегування, зберігання та осмислення даних.

8) Немає користі в даних про загрози, що надається відповідальним за реагування на інциденти.

Проблема: дані про загрози — це актуальна тема в IT-безпеці і продукти аналізу загроз стають дедалі більш популярними, але багато організацій виявляють, що придбання всіх доступних каналів загроз не призводить до повного виявлення загроз. Часто спеціалісти з реагування на інциденти перевантажені хешами, іменами файлів, IP-адресами та іншими індикаторами,

але їм майже або взагалі не надається контекст щодо того, як ці індикатори можуть вплинути на їхню організацію.

Вирішення: організації повинні інтегрувати інформацію про загрози в реагування на інциденти та активно співпрацювати зі своїм постачальником даних про загрози, щоб оцінити, чи є ця інформація дієвою та цінною.

9) Групі реагування на інциденти не вистачає авторитету та прозорості в організації.

Проблема: конфлікт інтересів та суперечки у колективі організації можуть перешкоджати зусиллям групи реагування на інциденти, перешкоджати процесу реагування та перешкоджати вчасному вирішенню інцидентів. Рідко трапляється так, що групи реагування на інциденти мають абсолютні повноваження вносити зміни в бізнес для забезпечення безпеки організації. Навпаки, вони повинні передавати проблеми керівництву, щоб отримати необхідні дозволи, що часто ускладнює процес реагування.

Вирішення: керівництво повинно повністю підтримувати групу реагування на інциденти та її діяльність під час розслідування. Реагування на інциденти слід повідомляти та рекламувати як послугу, яка підтримує цілісність організації, а не як групу, яка створює більше роботи. Крім того, група реагування на інциденти повинна залучати інші групи для сприяння участі в процесі реагування на інциденти.

10) Користувачі не знають про свою роль у забезпеченні безпеки організації.

Проблема: експлуатація користувачів є одним із найпоширеніших і найпростіших способів компрометації злочинцями організацій. Знайти вразливість, яка надає зловмиснику повний доступ до мережі, може бути дуже складно, але створити повідомлення електронної пошти, яке переконає користувача запустити зловмисне програмне забезпечення, — вкрай легко.

Вирішення: команда агентств з управління безпекою повинна постійно навчати користувачів не лише про загальні практики експлуатації, але й про роль інформаційної безпеки в організації. Таким чином користувачі можуть

бути активними учасниками безпеки. Вони знатимуть, куди звернутися, і довірятимуть процесу, а не намагатимуться вирішити проблеми безпеки самостійно, встановлюючи ненадійні інструменти та потенційно спричиняючи більші проблеми в мережі.

Також при побудові процесу реагування на інциденти інформаційної безпеки необхідно врахувати такі аспекти [6]:

1) Обсяг ризиків

Величезна кількість атак на кібербезпеку є однією з найбільших проблем, з якою стикається як галузь кібербезпеки в цілому, так і управління IT окремих компаній.

Згідно з одним із досліджень кібератак у 2020 році, 80 відсотків компаній повідомили про збільшення кількості кібератак порівняно з 2019 роком. Це число збільшується для окремих галузей, а банки спостерігають зростання на понад 238 відсотків.

Крім того, у першій половині 2020 року відбулися сплески певних типів атак:

- Фішингове шахрайство зросло на 600 відсотків з березня
- Хмарні атаки зросли на 630 відсотків у першому кварталі
- Кібератака відбувається приблизно кожні 39 секунд

Важливо зазначити, що не кожен інцидент перетворюється на успішну атаку, але кожна окрема спроба спочатку була інцидентом. Це означає, що загальна кількість інцидентів потенційно експоненціально перевищує навіть цифри вище.

Не дивно, що весь цей обсяг може бути занадто великим для компаній.

2) Вимоги до конфіденційності

Залежно від галузі, у якій працює організація, на неї може бути покладене зобов’язання відповідати низці нормативних вимог. Ці вказівки та протоколи можуть значно відрізнятися залежно від організації чи установи, які їх адмініструють і забезпечують дотримання.

Однак вони значною мірою збігаються, особливо коли йдеться про одну сферу - конфіденційність.

Компанії, відповідальні за зберігання, обробку або транспортування конфіденційної інформації про клієнтів, мають бути обережними щодо того, як вони це роблять. Наприклад, Закон про перенесення та підзвітність медичного страхування (HIPAA) вимагає суворих стандартів для будь-якої обробки особистої медичної інформації, як-от медичних записів. Подібним чином Стандарт безпеки даних індустрії платіжних карток (PCI-DSS) визначає правила обробки кредитної картки та іншої фінансової інформації клієнтів.

Відповідність нормативним вимогам є досить складною справою зі стабільними правилами. Крім того, ці стандарти з часом оновлюються у відповідь на атаки, вимагаючи постійного виправлення нещодавно застарілих елементів керування конфіденційністю. Ці змінні вимоги до конфіденційності ускладнюють дотримання вимог. Що ще важливіше, вони також становлять постійну загрозу для ефективного управління інцидентами.

3) Внутрішні загрози

Багато систем кібербезпеки базуються на припущенні, що атаки відбуваються ззовні, хоча це не обов’язково так.

Ще однією серйозною проблемою, яка перешкоджає успішному управлінню інцидентами, є той факт, що багато компаній погано оснащені для боротьби із загрозою атак зсередини. Деякі з найпоширеніших винних у кіберзлочинах – це ті, хто має привілейований доступ до мережі компанії.

Нижче наведено кілька прикладів осіб, які можуть здійснити внутрішні атаки:

- Незадоволені діючі або колишні працівники
- Підрядники, які отримали, здавалося б, тимчасовий доступ до систем
- Персонал, який мимоволі порушує протоколи безпеки

Згідно зі статистикою інсайдерських атак за 2020 рік, у США щодня відбувається близько 2500 порушень внутрішньої безпеки — трохи менше 1 мільйона на рік.

Ці внутрішні атаки щороку вражають більше третини всіх компаній у всьому світі. Дві третини вважають внутрішні загрози більш небезпечними, ніж зовнішні. Також внутрішні зловмисники можуть залишатися непоміченими довше, потенційно завдаючи набагато більше шкоди, ніж зовнішній хакер.

4) Інформаційні недоліки

Одним із найважливіших аспектів здатності компанії виявляти ризики та реагувати на них є інформація. Але в цьому полягає ключова проблема: збір, класифікація та обробка різноманітних даних, необхідних для ефективного управління інцидентами, може бути складною. Це особливо вірно для малих і середніх підприємств з меншою кількістю ресурсів, виділених на IT.

Найважливіша інформація, яку необхідно каталогізувати та оптимізувати для аналізу в реальному часі та прийняття рішень, включає:

- Розширений перелік усього апаратного забезпечення, яким володіє або керує компанія:
- Усі комп’ютери та IT-пристрої (мобільні телефони тощо)
- Усі сервери, комутатори та інші мережеві компоненти
- Усе програмне забезпечення, яке належить або використовується компанією:
- Додатки, браузери та програми
- Хмарні сховища та обчислювальні послуги
- Детальні записи щодо всього персоналу та обраної клієнтури

Важливо не тільки мати великі записи та легкий доступ до всіх даних; їх також потрібно захистити за допомогою автентифікації, шифрування та інших засобів. Для виявлення ризиків важливо знати, яка інформація є, де вона розташована та як швидко надати (або припинити) доступ до неї.

5) Бюджетні обмеження

Цей останній виклик є не такою окремою категорією, як основною причиною того, що всі інші виклики є викликами в першу чергу. Дуже часто програми управління інцидентами важко теоретизувати та реалізувати, оскільки організаціям бракує необхідного бюджету для IT.

Звіт Forbes про перспективи IT-бюджетів свідчить про те, що директори з інформаційних технологій (CIO) очікують зупинки зростання IT-бюджетів у всьому світі.

І, згідно зі звітом Wall Street Journal про витрати компаній на IT, ці скорочення бюджетів не використовуються для управління інцидентами. Натомість пріоритетом є хмарні сервіси та сервіси штучного інтелекту.

Ці скорочення очікуваних витрат на IT на практиці означають те, що відділи, які і так були розсіяні, тепер мають ще меншу пропускну здатність для всіх операцій кіберзахисту. Це включає в себе управління інцидентами, яке вже є складним через наведені вище причини.

1.2. Загальні засади побудови процесу реагування на інциденти інформаційної безпеки

Управління інцидентами безпеки – це процес ідентифікації, керування, документування та аналізу загроз або інцидентів безпеки в режимі реального часу, спрямований на забезпечення достовірного та повного уявлення про проблеми безпеки в IT-інфраструктурі. Інцидент безпеки може бути чим завгодно: від активної загрози до спроби вторгнення до успішної компрометації чи витоку даних. Порушення правил і несанкціонований доступ до таких даних, як медичні, фінансові номери, номери соціального страхування та особисті записи – усе це приклади інцидентів безпеки [7].

Оскільки обсяг і складність загроз кібербезпеці продовжують зростати, організації впроваджують методи, які дозволяють їм швидко виявляти, реагувати та пом’якшувати ці типи інцидентів, одночасно стаючи більш стійкими та захищаючи від майбутніх інцидентів.

Управління інцидентами безпеки використовує поєднання пристроїв, програмного забезпечення та ручного розслідування і аналізу. Процес управління інцидентами безпеки зазвичай починається з попередження про те, що стався інцидент, і залучення групи реагування на інциденти. Після цього

спеціалісти з реагування на інцидент досліджуватимуть і аналізуватимуть інцидент, щоб визначити його масштаб, оцінити збитки та розробити план пом’якшення наслідків.

Це означає, що багатогранна стратегія управління інцидентами безпеки повинна бути реалізована, щоб забезпечити справжню безпеку IT-середовища. Стандарт ISO/IEC 27035 описує п’ятиетапний процес управління інцидентами безпеки. Дані етапи включають:

1) Підготовка до врегулювання інцидентів.

2) Визначення потенційних інцидентів безпеки за допомогою моніторингу та повідомлення про всі інциденти.

3) Оцінка ідентифікованих інцидентів з метою визначення відповідних наступних кроків для зменшення ризику.

4) Реагування на інцидент, локалізація, розслідування та вирішення інциденту.

5) Вивчення та документування ключових висновків кожного інциденту.

Хоча заходи реагування на інциденти можуть відрізнятися залежно від організації та відповідних бізнес-функцій, існують загальні кроки, які часто вживаються для управління загрозами. Перший крок може початися з повного дослідження аномальної системи або порушення в системі, даних або поведінці користувача.

Наприклад, група управління інцидентами безпеки може визначити сервер, який працює повільніше, ніж зазвичай. Після цього команда оцінить проблему, щоб визначити, чи є поведінка результатом інциденту безпеки. Якщо це доведено, тоді інцидент буде проаналізовано додатково; інформація збирається та документується, щоб визначити масштаби інциденту та кроки, необхідні для вирішення, а також складається докладний звіт про інцидент безпеки.

У разі потреби можуть бути залучені правоохоронні органи. Якщо інцидент передбачає розкриття або крадіжку конфіденційних записів клієнтів,

тоді може бути зроблено публічне оголошення із залученням виконавчого керівництва та групи зв’язків із громадськістю.

Організації будь-якого розміру та типу повинні планувати процес управління інцидентами безпеки. Найкращі практики для розробки комплексного плану управління інцидентами безпеки включають такі пункти:

1) Розробка плану управління інцидентами безпеки та допоміжних політик, які включають вказівки щодо того, як виявляти інциденти, повідомляти, оцінювати та реагувати на них. Підготовка контрольного списку набору дій для кожного типу загрози. Постійне оновлення процедури управління інцидентами безпеки, зокрема з урахуванням уроків, отриманих із попередніх інцидентів.

2) Створення групи реагування на інциденти (іноді її називають CSIRT), включаючи чітко визначені ролі та обов’язки. Група реагування на інциденти має включати функціональні ролі у відділі IT/безпеки, а також представляти інші відділи, такі як юридичний, комунікаційний, фінансовий, а також управління бізнесом.

3) Розробка комплексної програми навчання для кожної діяльності, необхідної в рамках набору процедур управління інцидентами безпеки. Перевірка плану управління інцидентами безпеки за допомогою тестових сценаріїв на послідовній основі та внесення уточнень за потреби.

4) Проведення аналізу після будь-якого інциденту інформаційної безпеки для аналізу успіхів і невдач та за потреби внесення коректив у програму безпеки та процес керування інцидентами.

У деяких ситуаціях збір доказів і аналіз криміналістики є необхідним компонентом реагування на інцидент. Для цього необхідно забезпечити такі процедури і фактори:

1) Розробка політики щодо збору доказів, яка забезпечує їх правильність та доступність і достовірність для використання в суді за необхідності.

2) Здатність використовувати криміналістику за потреби для аналізу, звітності та розслідування.

3) Члени команди, які мають досвід і підготовку в галузі криміналістики та функціональних методів.

Надійний процес управління інцидентами безпеки є обов'язковим для зменшення витрат на відновлення, потенційних зобов'язань і шкоди організації-жертві. Організації повинні оцінити та вибрати набір інструментів для покращення видимості, оповіщення та можливості вжиття заходів щодо інцидентів безпеки [7].

Таким чином побудова системи управління інцидентами інформаційної безпеки є складним процесом і включає велику кількість аспектів [8]:

- Визначення цілі управління інцидентами інформаційної безпеки в організації;
- Визначення можливих типів інцидентів;
- Побудова системи відповідно до світових стандартів з управління інцидентами;
- Визначення основних процесів системи управління інцидентами інформаційної безпеки;
- Розробка робочої документації.

Отже основною задачею управління інцидентами інформаційної безпеки можна визначити оперативне відновлення нормальної роботи підприємства і звести до мінімуму негативний вплив інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні [8].

Цілі управління інцидентами [9]:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх інцидентів інформаційної безпеки і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливих напрямках;

- надання відомостей, які роблять можливим оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Управління інцидентами і проблемами інформаційної безпеки є комплексним рішенням, що оптимізує управління всіма аспектами обслуговування і підтримки, необхідними для підприємства. Використовуючи кращі, перевірені часом, напрацювання і відновлення IT-процесів після збоїв будь-яких видів, рішення з управління інцидентами інформаційної безпеки дозволяють використовувати ресурси залежно від пріоритетів бізнес-діяльності, управляти рівнями обслуговування, а також краще контролювати витрати IT-служб. Рішення з управління інцидентами інформаційної безпеки прискорює процеси реагування на інциденти інформаційної безпеки на всіх етапах: від первинного виявлення і діагностики проблем та основних причин до остаточного їх усунення [10].

Основними заходами створення системи управління інцидентами інформаційної безпеки є [10]:

1) Виділення ресурсів для розробки та впровадження системи управління інцидентами інформаційної безпеки.

2) Визначення сфери функціонування системи управління інцидентами інформаційної безпеки.

3) Розробка комплексу процесів системи управління інцидентами інформаційної безпеки.

4) Навчання персоналу.

5) Впровадження процесів управління інцидентами інформаційної безпеки та їх інтегрування з функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності.

6) Розробка архітектури і комплексу технічних засобів з автоматизації процесів управління інцидентами інформаційної безпеки і моніторингу подій інформаційної безпеки.

7) Впровадження комплексу програмно-технічних засобів автоматизації управління інцидентами інформаційної безпеки.

Альтернативна інтерпретація кроків побудови системи управління інцидентами інформаційної безпеки наведена на Рис. 1.2.1.

Рис. 1.2.1. Етапи побудови системи управління інцидентами інформаційної безпеки

Основні три етапи – інвентаризація, оцінка та оптимізація, деталізовано наступними кроками [11]:

1) Інвентаризація активів.

2) Інвентаризація бізнес-процесів, що використовують ці активи.

3) Визначення, які з бізнес-процесів є критичними.

4) Інвентаризація загроз.

5) Визначення вразливостей, через які існуючі загрози можуть реалізовуватись.

6) Оцінка ймовірності реалізації описаних загроз стосовно активів, які є стратегічно важливими для бізнесу.

7) Оцінка впливу актуальних загроз на активи, а через них і безпосередньо на критичні бізнес-процеси.

8) Розробка планів мінімізації ризиків реалізації загроз.

9) Виконання цих планів у встановлені терміни, та по можливості, з бажаними наслідками.

10) Оцінка, наскільки співпадають наслідки виконання планів з очікуваннями.

11) Внесення коригувань у плани.

12) Повторення процесу з початку.

Результатом зазначених заходів буде впровадження системи управління інцидентами інформаційної безпеки, яка буде вирішувати такі завдання [12]:

1) Оперативний моніторинг стану інформаційної безпеки в межах обраної сфери дії системи управління інцидентами інформаційної безпеки.

2) Виявлення, облік, реагування, розслідування та аналіз інцидентів інформаційної безпеки.

3) Інформування вищого керівництва і зацікавлених осіб про поточний стан інформаційної безпеки.

Також, слід зазначити, що при експлуатації різного роду системи управління інформаційною безпекою процес управління інцидентами інформаційної безпеки є одним з найважливіших постачальників даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування удосконалення роботи системи [10].

1.3. Стандарти організації процесу управління інцидентами інформаційної безпеки

Специфічні питання управління інцидентами інформаційної безпеки розглядаються та регламентуються такими міжнародними та національними нормативними документами: ISO 20000, ISO/IEC 27001, ISO/IEC 27035, CMU/SEI-2004-TR-015, NIST SP 800-16, ITU-T X-1051, ITU-T E.409 [9]. Далі в роботі розглянуто декілька з них – останню редакцію ISO/IEC 27035-3:2020 та NIST SP 800-61.

1.3.1. Процес управління інцидентами інформаційної безпеки відповідно до стандарту ISO/IEC 27035

У стандарті ISO/IEC 27035-3:2020 наведено рекомендації щодо реагування на інциденти інформаційної безпеки в операціях безпеки інформаційно-комунікаційних технологій. Цей документ, по-перше, висвітлює оперативні аспекти операцій безпеки інформаційно-комунікаційних технологій з точки зору людей, процесів і технологій. Далі він зосереджується на реагуванні на інциденти інформаційної безпеки в операціях з безпеки інформаційно-комунікаційних технологій, включаючи виявлення інцидентів інформаційної безпеки, звітування, обробку, аналіз, реагування, попередження, відповідь, відновлення та висновки, як наведено на Рис. 1.3.1.

Цей стандарт не стосується операцій з реагування на інциденти, не пов’язані з інформаційно-комунікаційних технологій (як втрата паперових документів).

Цей стандарт базується на фазі «Виявлення та звітування», фазі «Оцінка та прийняття рішення» та фазі «Відповіді» моделі «Фази управління інцидентами інформаційної безпеки», представлених у ISO/IEC 27035-1:2016.

Принципи, наведені в цьому стандарті, є загальними і призначені для застосування до всіх організацій, незалежно від типу, розміру або характеру. Організації можуть коригувати положення, наведені в цьому документі, відповідно до свого типу, розміру та характеру бізнесу у зв’язку з ситуацією ризику інформаційної безпеки.

Стандарт ISO/IEC 27035 також застосовується зовнішніх організацій, що надають послуги з управління інцидентами інформаційної безпеки [13].

Повний текст стандарту ISO/IEC 27035 доступний до завантаження за посиланням [14].

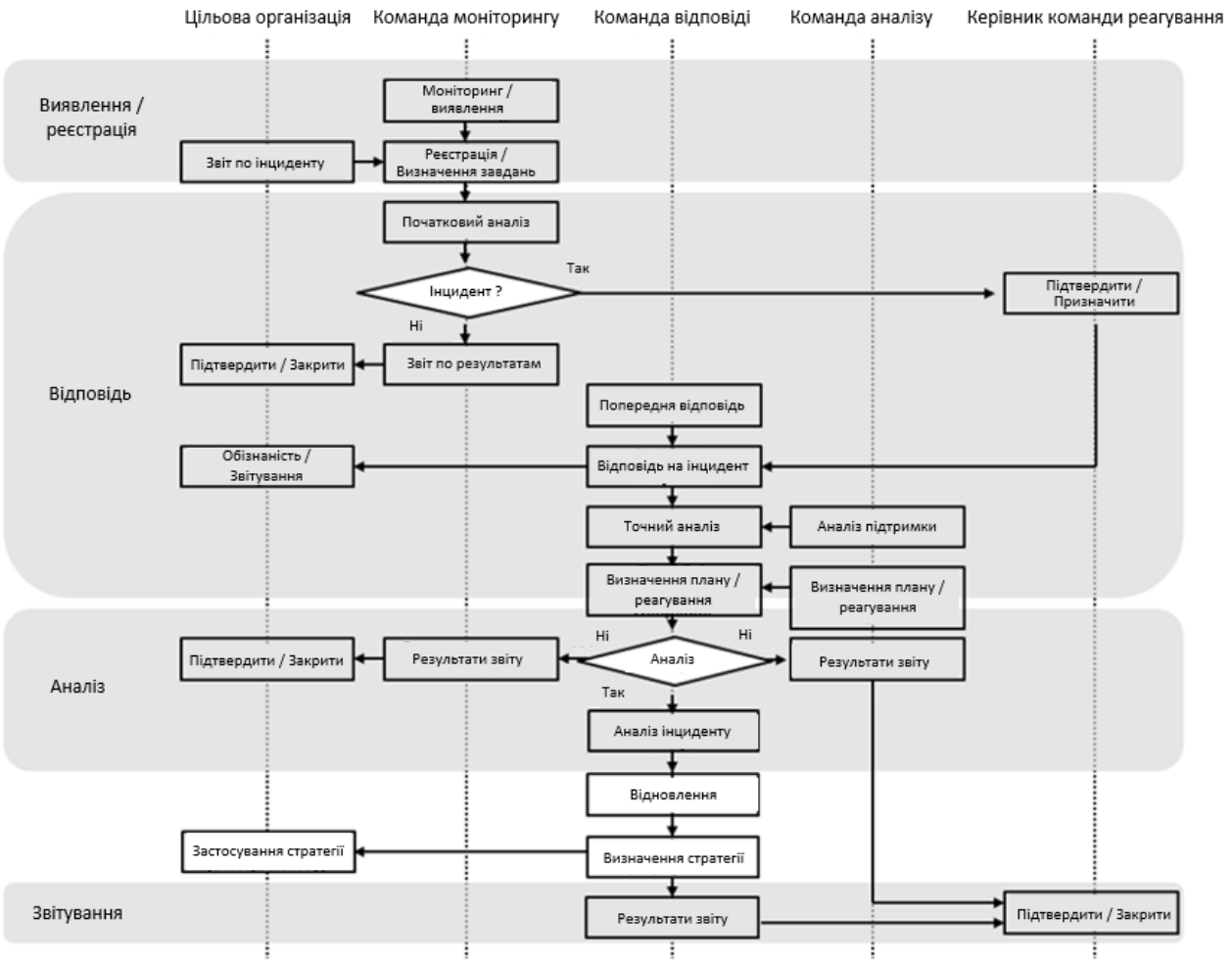

Рис. 1.3.1. Процес управління інцидентами інформаційної безпеки згідно з ISO/IEC 27035 1 [14]

Відповідно до розглянутого стандарту, процес управління інцидентами інформаційної безпеки зводиться до таких етапів [14]:

1. Виявлення і звітування про інциденти інформаційної безпеки.
    1. виявлення інцидентів;
    2. звітування.
2. Оцінка інцидентів інформаційної безпеки.
    1. оцінка та початкове рішення щодо обробки інциденту;
    2. оцінка і підтвердження інциденту командою реагування на інциденти.
3. Відповідь на інцидент інформаційної безпеки.
    1. негайна відповідь;

2. оцінка контролю інциденту інформаційної безпеки;
3. подальша відповідь на інцидент;
4. реагування в кризових ситуаціях;
5. криміналістичний аналіз інформаційної безпеки;
6. комунікації при розслідуванні інциденту;
7. ескалація;
8. реєстрація діяльності та контроль змін.

Деталізовані етапи процесу управління інцидентами інформаційної безпеки:

1. Виявлення інцидентів інформаційної безпеки

Події інформаційної безпеки можуть бути виявлені безпосередньо особою або особами, які помітили події, які викликає занепокоєння, технічні, фізичні чи процедурні. Виявлення може здійснюватися, наприклад, за допомогою сповіщувачів пожежі/диму або зловмисної сигналізації, при цьому оповіщення сповіщаються в заздалегідь визначених місцях для дій людини. Події безпеки технічної інформації можуть бути виявлені за допомогою автоматичних засобів, наприклад, попереджень за допомогою засобів аналізу слідів аудиту, брандмауерів, систем виявлення вторгнень та засобів захисту від шкідливого коду (включаючи віруси), у кожному випадку стимульованих попередньо встановленими параметрами [14].

Можливі джерела виявлення подій інформаційної безпеки включають:

- користувачі;
- лінійні керівники та менеджери з безпеки;
- клієнти;
- ІТ-відділ, включаючи центр мережевих операцій та операційний центр безпеки (через підтримку 2-го рівня);
- ІТ-довідкова служба (через підтримку 1-го рівня);
- постачальники керованих послуг (включаючи постачальників послуг Інтернету, постачальників телекомунікаційних послуг та постачальників);
- команди відповіді на інциденти;

- інші підрозділи та персонал, які можуть виявити аномалії під час щоденної роботи;
- засоби масової інформації;
- веб-сайти (веб-сайти з публічною інформацією про безпеку, веб-сайти дослідників безпеки тощо).

2. Звітування про інциденти інформаційної безпеки

Незалежно від джерела виявлення події інформаційної безпеки, особа, повідомлена за допомогою автоматичних засобів або безпосередньо помітила щось незвичайне, несе відповідальність за ініціювання процесу виявлення та звітування. Це може бути будь-який член персоналу організації, як постійний, так і за контрактом.

Особа повинна дотримуватися процедур і використовувати форму звіту про події інформаційної безпеки, визначену схемою управління інцидентами інформаційної безпеки, щоб довести подію інформаційної безпеки до відома керівництва. Відповідно, важливо, щоб весь персонал був добре обізнаний і мав доступ до інструкцій щодо звітування про різні типи можливих подій інформаційної безпеки. Це включає в себе формат форми звіту про події інформаційної безпеки та відомості про персонал, якого слід повідомляти щоразу (увесь персонал повинен принаймні знати формат форми звіту про інциденти інформаційної безпеки). Слід зазначити, що стаціонарний телефон, бездротовий телефон і мобільний телефон без захисту від прослуховування вважаються небезпечними. При роботі з дуже конфіденційною або секретною інформацією слід вживати додаткових заходів безпеки.

В якості основи для форми системи відстеження інцидентів може бути використана така інформація [14]:

- час/дата виявлення;
- спостереження;
- контактна інформація (необов’язково).

Заповнена форма (як у паперовій, так і в електронній формі) повинна використовуватися персоналом команди реагування на інциденти лише під час реєстрації подій інформаційної безпеки (можливо інцидентів) або вразливостей у системі відстеження інцидентів. Важливіше отримати знання/звіти про підозрювану/пережиту/виявлену подію інформаційної безпеки, ніж повну інформацію.

Відстеження подій (можливо, інцидентів) інформаційної безпеки має підтримуватися, якщо це можливо, автоматичною програмою. Використання інформаційної системи має важливе значення, щоб змусити персонал дотримуватися встановлених процедур і контрольних списків. Також надзвичайно корисно відстежувати «хто, що і коли зробив», деталі, які можуть бути упущені помилково під час події інформаційної безпеки (можливо, інциденту) [14].

Спосіб обробки події інформаційної безпеки залежить від того, що вона собою представляє, а також від наслідків, які можуть випливати з цього. Для багатьох людей це буде рішення за межами їх компетенції. Таким чином, особа, яка повідомляє про подію інформаційної безпеки, повинна заповнити форму звіту про подію інформаційної безпеки, вказавши стільки опису та іншої інформації, яка доступна на даний момент, зв’язуючись зі своїм місцевим керівником, якщо це необхідно. Цю форму слід надійно передати до відповідального з команди реагування на інциденти.

Команда реагування на інциденти має призначити одного члена команди або делегата на зміну, щоб відповідати за всі вхідні звіти через електронну пошту, телефон, факс, програми автоматизованого обміну інформацією, форми та пряму розмову. Ця відповідальність може змінюватися між членами команди щотижня. Призначений член команди проводить оцінку та вживає відповідних дій для інформування відповідальних та залучених сторін, а також вирішення інциденту інформаційної безпеки.

Наголошується, що важлива не лише точність, а й своєчасність змісту, заповненого у формі звіту про події інформаційної безпеки. Неправильно

відкладати подачу звітної форми, щоб підвищити точність її змісту. Якщо особа, яка звітує, не впевнена в даних у будь-якому полі у формі звітності, її слід подати з відповідними позначками, а зміни повідомити пізніше.

Формати даних автоматичного обміну інформацією (IETF RFC 5070) і протоколи (IETF RFC 6545, IETF RFC 6546) забезпечують рейтинг довіри до даних, що спільно використовують. Рейтинг довіри в поєднанні з інформацією про організацію, яка підтверджує дані, слід враховувати для визначення точності та оцінки наданої інформації.

Слід також визнати, що деякі механізми звітності (наприклад, електронна пошта, автоматизовані протоколи обміну інформацією) самі є видимими мішенями для атаки. Коли існують або наявні підозри про проблеми з електронними механізмами звітності (наприклад, електронною поштою), слід використовувати альтернативні засоби зв’язку. Це стосується випадків, коли вважається можливим, що система піддається атаці, і неавторизовані люди можуть прочитати електронні форми звітності. Альтернативні засоби можуть включати передачу звіту особисто, по телефону або надсилання текстових повідомлень. Такі альтернативні засоби слід використовувати, зокрема, коли на початку розслідування стає очевидним, що подія інформаційної безпеки може бути класифікована як інцидент інформаційної безпеки, особливо той, який може бути значущим.

Хоча в багатьох випадках про подію інформаційної безпеки потрібно повідомляти далі, можуть бути випадки, коли подія інформаційної безпеки обробляється локально, можливо, за допомогою місцевого керівництва. Бажано, щоб місцеве керівництво було навчене робити таку ж оцінку, що й команда реагування на інциденти, і вживати подібних контрзаходів, а також використовувати ту саму систему відстеження інцидентів, щоб успішно використовувати місцеві ресурси. Це запобіжить повторній роботі команди реагування на інцидент.

Подія інформаційної безпеки може бути швидко визначена як помилкова тривога, або вона може бути вирішена до задовільного висновку. У таких

випадках форму звітності слід заповнити та надіслати місцевому керівництву та команді реагування на інциденти для запису, тобто в базу даних подій/інцидентів/уразливостей інформаційної безпеки. За таких обставин особа, яка повідомляє про закриття події інформаційної безпеки, може мати змогу заповнити деяку інформацію, необхідну для форми звіту про інциденти інформаційної безпеки – якщо це так, то форму звіту про інцидент інформаційної безпеки також слід заповнити та надіслати. Використання автоматичних інструментів може допомогти із заповненням деяких полів, наприклад відмітки часу. Це також може допомогти з обміном\передачею необхідної інформації [14].

3. Оцінка інциденту інформаційної безпеки та вживання початкових заходів

Приймаюча особа має підтвердити отримання заповненої форми звіту про події інформаційної безпеки, ввести її в базу даних подій/інцидентів/уразливостей інформаційної безпеки та переглянути її. Він/вона повинен отримати будь-які роз’яснення від особи, яка повідомляє про подію із інформаційної безпеки, і зібрати будь-яку додаткову інформацію, яка потрібна та, як відомо, є доступною, чи то від особи, яка повідомляє, чи в іншому місці. Потім відповідальна особа має провести оцінку, щоб визначити, чи слід класифікувати подію інформаційної безпеки як інцидент інформаційної безпеки чи це насправді помилкова тривога (включаючи використання узгодженої організації шкали класифікації інцидентів). Якщо визнається, що подія інформаційної безпеки є помилковою тривогою, форму звіту про подію інформаційної безпеки слід заповнити та надіслати до команди реагування на інциденти для додавання до бази даних подій/інцидентів/вразливостей інформаційної безпеки та перегляду та скопіювати особі, яка повідомляє, та її локальному корівнику.

Інформація та інші докази, зібрані на цьому етапі, можливо, знадобиться використовувати в майбутньому для дисциплінарного чи судового розгляду.

Особа або люди, які виконують завдання зі збору та оцінки інформації, повинні бути навчені вимогам збору та збереження доказів.

На додаток до запису дати(-й) та часу(-ів) дій, необхідно повністю задокументувати наступне [14]:

- що було помічено та зроблено (включаючи використані інструменти) і чому;
- місцезнаходження потенційних доказів;
- як архівуються докази (якщо вони наявні);
- як проводилась перевірка доказів (якщо застосовно);
- деталі зберігання/безпечного зберігання матеріалу та подальший доступ до нього.

Якщо подія інформаційної безпеки визначається як ймовірний інцидент інформаційної безпеки, і якщо відповідальна особа має відповідний рівень компетентності, може бути проведена додаткова оцінка. Це може вимагати заходів з виправлення ситуації, наприклад визначення додаткових засобів контролю над надзвичайними ситуаціями та направлення відповідної особи для виконання заходів. Може бути очевидним, що подія інформаційної безпеки визначається як небезпечний інцидент інформаційної безпеки (з використанням заздалегідь визначеної шкали серйозності організації), у цьому випадку слід повідомити безпосередньо керівника команди реагування на інциденти. Може бути очевидним, що кризову ситуацію слід оголосити, і, наприклад, повідомити менеджера з антикризового управління про можливу активацію плану антикризового управління, а також повідомити керівника команди реагування на інциденти та вище керівництво. Однак найімовірніша ситуація полягає в тому, що інцидент інформаційної безпеки необхідно направити безпосередньо до команди реагування на інциденти для подальшої оцінки та дій.

Яким би не був визначений наступний крок, відповідальна особа має заповнити якомога більш детально форму звіту про інциденти інформаційної безпеки. Форма звіту про інциденти інформаційної безпеки повинна містити опис і, наскільки це можливо, підтверджувати та описувати наступне [14]:

- опис даного інциденту інформаційної безпеки;
- як він був викликаний і чим або ким;
- на що він впливає або може вплинути;
- вплив або потенційний вплив інциденту інформаційної безпеки на бізнес організації;
- вказівку на те, чи вважається інцидент інформаційної безпеки значним чи ні (з використанням попередньо визначеної шкали класифікації організації);
- яка ситуація була до виникнення інциденту.

Перший крок полягає в тому, щоб розглянути, який із ряду наслідків має значення. Для тих, які вважаються релевантними, слід використовувати рекомендації щодо пов’язаних категорій для встановлення потенційних або фактичних впливів для внесення до звіту про інциденти інформаційної безпеки. Приклади категорій [14]:

- фінансові втрати/зриви господарських операцій;
- комерційні та економічні інтереси;
- особиста інформація;
- юридичні та нормативні зобов'язання;
- управління та господарські операції;
- втрата репутації;
- поранення або втрата життя;
- соціальні порушення.

Якщо інцидент інформаційної безпеки було вирішено, звіт повинен містити детальну інформацію про вжиті засоби контролю та будь-які винесені уроки (наприклад, засоби контролю, які необхідно застосувати для запобігання повторенню чи подібним подіям). Після заповнення, наскільки це можливо, форму звітності слід направити до команди реагування на інциденти для внесення до бази даних подій/інцидентів/уразливостей інформаційної безпеки та перегляду.

Якщо розслідування, ймовірно, буде довшим за період часу, визначений у політиці управління інцидентами інформаційної безпеки, проміжний звіт має бути складений протягом періоду часу, визначеного політикою.

Наголошується, що відповідальна особа, яка оцінює інцидент інформаційної безпеки, повинна ґрунтуватись на вказівках, наданих у документації щодо схеми управління інцидентами інформаційної безпеки [14].

4. Оцінка та підтвердження інциденту інформаційної безпеки командою реагування на інциденти

Оцінка та підтвердження рішення щодо того, чи слід класифікувати подію інформаційної безпеки як інцидент інформаційної безпеки, має бути прийнято відповідальним команди реагування на інциденти. Приймаюча особа в команді реагування на інциденти повинна зробити наступне [14]:

- підтвердити отримання форми звіту про інциденти інформаційної безпеки;
- ввести форму в базу даних подій/інцидентів/вразливостей інформаційної безпеки та оновити базу даних, якщо необхідно;
- за потреби звернутися за роз’ясненнями до особи, що звітувала попередньо;
- переглянути зміст форми звітності;
- зібрати будь-яку додаткову інформацію, необхідну та, як відомо, доступну, чи то від особи, яка заповнила форму звіту про події інформаційної безпеки, чи в іншому місці;

Інцидент інформаційної безпеки слід співвідносити з будь-якою іншою подією/інцидентом, про яку повідомляється команді реагування на інциденти. Ця важлива діяльність полягає в тому, щоб перевірити, чи пов’язаний інцидент з будь-якою іншою подією/інцидентом, чи це просто результат іншого інциденту, наприклад, в результаті атак «Відмова в обслуговуванні» (DoS) та «Розподілена відмова в обслуговуванні» (DDoS). Співвідношення інцидентів

також важливе для визначення пріоритетів зусиль команди реагування на інциденти.

Якщо визнається, що інцидент інформаційної безпеки є реальним, відповідальний з команди реагування на інциденти та його колеги, якщо потрібно, повинні провести додаткову оцінку. Мета полягає в тому, щоб якомога швидше підтвердити наступне [14]:

- в чому полягає виявлений інцидент інформаційної безпеки, як він був викликаний і чим або ким, на що він впливає або може вплинути, вплив або потенційний вплив інциденту інформаційної безпеки на бізнес організації, вказівка на те, чи інформація інцидент безпеки вважається значущим чи ні (з використанням заздалегідь визначеної організації шкали серйозності). Якщо інцидент завдає серйозного негативного впливу на бізнес, слід розпочати діяльність при кризових ситуаціях;
- наведені нижче аспекти навмисної технічної атаки людини на інформаційну систему, службу та/або мережу, наприклад:
    - наскільки глибоко проникли в систему, службу та/або мережу та який рівень контролю має зловмисник,
    - до яких даних отримав доступ зловмисник, які дані можливо скопійовані, змінені чи знищені;
    - яке програмне забезпечення було скопійовано, змінено або знищено зловмисником;
- прямі та непрямі наслідки (наприклад, фізичний доступ відкритий через пожежу, інформаційна система вразлива через несправність якогось програмного забезпечення або лінії зв'язку або через людську помилку);
- як і ким розглядався інцидент інформаційної безпеки.

При розгляді потенційних або фактичних негативних наслідків інциденту інформаційної безпеки на бізнес організації, необхідно підтвердити, який із ряду наслідків є релевантним.

Процес визначення пріоритетів повинен використовуватися для призначення інциденту інформаційної безпеки найбільш підходящій особі або

групі осіб у команді реагування на інциденти, щоб полегшити адекватну відповідь на інцидент інформаційної безпеки. Зокрема, коли розглядаються кілька інцидентів інформаційної безпеки одночасно, необхідно встановити пріоритети, щоб упорядковувати відповіді на інциденти інформаційної безпеки.

Пріоритети мають бути встановлені відповідно до визначених негативних впливів на бізнес, пов’язаних із інцидентом інформаційної безпеки, та оцінених зусиль, необхідних для реагування на інцидент інформаційної безпеки. Для інцидентів з однаковим пріоритетом необхідні зусилля – це один показник, щоб визначити порядок, у якому на них потрібно реагувати. Наприклад, інцидент, який легко вирішується, може бути розглянутий до як інциденту, що вимагає більших зусиль.

Для інциденту, що вважається релевантним, слід використовувати рекомендації щодо пов’язаних категорій для встановлення потенційних або фактичних впливів для внесення до звіту про інциденти інформаційної безпеки [14].

5. Негайна відповідь на інцидент інформаційної безпеки

У більшості випадків наступні дії для члена команди реагування на інциденти полягають у визначенні дій негайного реагування для подолання інциденту інформаційної безпеки, запису деталей у форму інциденту інформаційної безпеки та в базі даних подій/інцидентів/вразливостей інформаційної безпеки та повідомлення при необхідні дії відповідним особам або групам. Це може призвести до надзвичайних засобів контролю (наприклад, відключення/вимкнення постраждалої інформаційної системи, служби та/або мережі за попередньою згодою відповідного IT та/або керівництва бізнесу) та/або виявлення додаткових постійних засобів контролю, і повідомлено про дії відповідної особи або групи. Якщо це ще не зроблено, значення інциденту інформаційної безпеки має бути визначено, використовуючи заздалегідь визначену шкалу класифікації організації, і, якщо є достатньо значущим,

відповідне вище керівництво має бути повідомлено безпосередньо. Якщо очевидно, що кризову ситуацію слід оголосити, наприклад, менеджера з антикризового управління слід повідомити про можливу активацію плану антикризового управління, а також повідомити керівника команди реагування на інциденти та вище керівництво.

Загальними цілями реагування на інциденти інформаційної безпеки є наступні: обмежити потенційні негативні наслідки (інцидентів інформаційної безпеки), і покращити інформаційну безпеку.

Основною метою схеми управління інцидентами інформаційної безпеки та пов’язаних з нею заходів має бути мінімізація негативного впливу на бізнес, тоді як виявлення зловмисника має розглядатися як другорядна мета.

Як приклад відповідних дій негайного реагування у разі навмисної атаки на інформаційну систему, службу та/або мережу, її можна залишити підключеною до Інтернету чи іншої мережі. Це дозволить критичним для бізнесу програмам функціонувати правильно та збирати якомога більше інформації про зловмисника, за умови, що зловмисник не знає, що він/вона знаходиться під наглядом.

Дуже важливо дотримуватися запланованих процесів і записувати дії. Остерігайтеся троянських програм, руткітів і модулів ядра, які можуть завдати серйозної шкоди системі. Докази можна захистити за допомогою криптографії, замків і записів доступу.

Приймаючи таке рішення, необхідно враховувати, що зловмисник може усвідомити, що за ним/нею спостерігають, і може вчинити дії, які завдають подальшої шкоди постраждалій інформаційній системі, службі та/або мережі та пов’язаним з нею даним, і зловмисник може знищити інформацію, яка може бути корисною для його/її відстеження.

Важливо, щоб було технічно можливо швидко та надійно відключити та/або вимкнути інформаційну систему, що зазнала атаки, службу та/або мережу після прийняття рішення. Це служить для стримування інциденту.

Подальше міркування полягає в тому, що запобігання повторному виникненню, як правило, має високий пріоритет, і цілком можна зробити висновок, що зловмисник виявив уразливість, яку слід виправити, а вигоди від його/неї відстеження не виправдовують зусиль, тому. Це особливо актуально, коли зловмисник не є зловмисним і завдав незначної шкоди або взагалі не завдав.

Що стосується інцидентів інформаційної безпеки, які спричинені чимось іншим, ніж навмисна атака, джерело слід визначити. Може знадобитися вимкнути інформаційну систему, службу та/або мережу, або ізолювати відповідну частину та вимкнути її (за попередньою згодою відповідного IT та/або керівництва бізнесу), під час впровадження контролю. Це може зайняти більше часу, якщо вразливість є фундаментальною для інформаційної системи, служби та/або мережі, або якщо це критична вразливість.

Іншою діяльністю реагування може бути активація методів нагляду (наприклад, honeypots). Це має відбуватися на основі процедур, задокументованих для схеми управління інцидентами інформаційної безпеки.

Щодо інформації, яка може бути пошкоджена в результаті інциденту інформаційної безпеки, член команди реагування на інциденти повинен перевірити резервні записи на предмет змін, видалення або вставлення інформації. Можливо, знадобиться перевірити цілісність журналів, оскільки навмисний зловмисник міг маніпулювати цими журналами, щоб прикрити свої сліди [14].

6. Оновлення даних про інцидент інформаційної безпеки

Яким би не був визначений наступний крок, член команди реагування на інциденти повинен якомога більше оновити звіт про інциденти інформаційної безпеки, додати його до бази даних подій/інцидентів/вразливостей інформаційної безпеки та повідомити менеджера команди реагування на інциденти та інших, якщо необхідно.

Важливо, що команда реагування на інциденти несе відповідальність за забезпечення безпечного збереження всієї інформації, що стосується інциденту інформаційної безпеки, для подальшого аналізу та потенційного використання юридичних доказів. Наприклад, для інциденту інформаційної безпеки, орієнтованого на IT, слід виконати наступні дії [14]:

1) Після первинного виявлення інциденту всі нестабільні дані повинні бути зібрані до того, як уражена IT-система, служба та/або мережа буде вимкнена, для повного розслідування криміналістичної експертизи інформаційної безпеки. Інформація, яку потрібно зібрати, включає вміст пам’яті, кешу та регістрів, а також подробиці будь-яких виконуваних дій.
2) Залежно від характеру інциденту інформаційної безпеки слід виконати повне дублювання криміналістичної експертизи ураженої системи або резервне копіювання журналів та важливих файлів низького рівня.
3) Слід збирати та переглянути журнали з сусідніх систем, служб і мереж, наприклад з маршрутизаторів і брандмауерів.
4) Уся зібрана інформація має надійно зберігатися на носіях, які доступні тільки для зчитування.
5) Дві або більше осіб повинні бути присутніми під час дублювання криміналістичної експертизи інформаційної безпеки, щоб підтвердити, що всі дії були здійснені відповідно до відповідного законодавства та нормативних актів.
6) Специфікації та описи інструментів і команд, які використовуються для дублювання криміналістичної експертизи інформаційної безпеки, повинні бути задокументовані та зберігатися разом з оригінальним носієм.

Член команди реагування на інциденти також несе відповідальність за сприяння поверненню постраждалого об’єкта (чи то IT, чи іншим чином) у безпечний робочий стан, який не піддається компрометації за допомогою тієї ж атаки, якщо це можливо на даному етапі [14].

7. Подальша обробка інциденту інформаційної безпеки

Якщо член команди реагування на інциденти визначає, що інцидент інформаційної безпеки є реальним, то інші важливі дії мають бути такими [10]:

- діяльність із запровадження криміналістичного аналізу інформаційної безпеки;
- діяльність щодо інформування відповідальних за внутрішні та зовнішні комунікації про факти і пропозиції щодо того, що, у якій формі та кому має бути повідомлено.

Якщо розслідування, ймовірно, триватиме більше, ніж період часу, попередньо узгоджений в організації, слід підготувати проміжний звіт.

Дії члену команди реагування на інциденти, який реагує на інцидент інформаційної безпеки, повинні засновуватись на вказівках, наданих у документації щодо схеми управління інцидентами інформаційної безпеки [14].

8. Оцінка контролю за інцидентами інформаційної безпеки

Після того, як член команди реагування на інциденти ініціював негайну відповідь та відповідну криміналістичну діяльність з аналізу інформаційної безпеки та комунікацій, необхідно швидко з’ясувати, чи інцидент інформаційної безпеки знаходиться під контролем. У разі необхідності член команди реагування на інциденти може проконсультуватися з колегами, керівником команди реагування на інциденти та/або іншими особами чи групами.

Якщо підтверджено, що інцидент інформаційної безпеки знаходиться під контролем, член команди реагування на інциденти повинен запровадити будь-які необхідні пізніші відповіді, а також криміналістичний аналіз інформаційної безпеки та комунікації, щоб припинити інцидент інформаційної безпеки та відновити інформаційну систему, яка постраждала, до нормального функціонування.

Якщо інцидент інформаційної безпеки підтверджується як неконтрольований, то член команди реагування на інциденти повинен розпочати кризову діяльність.

Якщо інцидент інформаційної безпеки пов’язаний із втратою доступності, показником для оцінки того, чи інцидент інформаційної безпеки контролюється, може бути час, що минув до відновлення нормальної ситуації після виникнення інциденту інформаційної безпеки. Організація повинна визначити для кожного активу на основі результатів оцінки ризику інформаційної безпеки його прийнятне вікно переривання, яке підтримує ціль часу відновлення до відновлення служби або доступу до інформації. Як тільки відповідь перевищить допустиме вікно переривання цільового активу, інцидент інформаційної безпеки може більше не перебувати під контролем, і слід прийняти рішення про ескалацію інциденту інформаційної безпеки.

Інциденти інформаційної безпеки, пов’язані з втратою конфіденційності, цілісності тощо, потребують інших типів суджень, щоб визначити, чи ситуація під контролем, і визначити можливі пов’язані показники відповідно до планів управління кризовими ситуаціями організації [14].

9. Подальша відповідь на інцидент інформаційної безпеки

Визначивши, що інцидент інформаційної безпеки знаходиться під контролем і не підлягає кризовій діяльності, член команди реагування на інциденти повинен визначити, чи потрібні подальші відповіді для вирішення інциденту інформаційної безпеки. Це може включати відновлення ураженої інформаційної системи (систем), служби (служб) та/або мережі (мереж) до нормальної роботи. Потім він/вона має записати деталі у формі звіту про інциденти інформаційної безпеки та в базі даних подій/інцидентів/вразливостей інформаційної безпеки та повідомити відповідальних за виконання відповідних дій. Після успішного виконання цих дій деталі мають бути записані у форму звіту про інциденти інформаційної безпеки та в базу даних подій/інцидентів/вразливостей інформаційної безпеки, а потім інцидент інформаційної безпеки слід закрити та повідомити відповідний персонал.

Далі можуть бути вжити деякі відповіді спрямовані на запобігання повторному виникненню інцидентів інформаційної безпеки або подібних

випадків. Наприклад, якщо буде встановлено, що причиною інциденту інформаційної безпеки є несправність апаратного чи програмного забезпечення ІТ без доступного виправлення, слід негайно зв'язатися з постачальником. Якщо відома вразливість ІТ була залучена до інциденту інформаційної безпеки, її слід виправити за допомогою відповідного оновлення інформаційної безпеки. Необхідно вирішувати будь-які проблеми, пов'язані з конфігурацією ІТ, на які випливає інцидент інформаційної безпеки після цього. Інші заходи щодо зменшення ймовірності повторення або подібних випадків інциденту ІТ-інформаційної безпеки можуть включати зміну системних паролів та відключення невикористаних служб.

Інша сфера реагування може включати моніторинг ІТ-системи, служби та/або мережі. Після оцінки інциденту інформаційної безпеки може бути доречним запровадити додаткові засоби контролю, щоб допомогти у виявленні незвичайних і підозрілих подій, які були б симптомами подальших інцидентів інформаційної безпеки. Такий моніторинг також може виявити більш глибокий інцидент інформаційної безпеки та виявити інші ІТ-системи, які були скомпрометовані.

Це може знадобитися для активізації конкретних реакцій, задокументованих у відповідному плані управління кризою. Це може стосуватися як ІТ, так і не пов'язаних із ІТ інцидентів інформаційної безпеки. Такі відповіді мають включати відповіді для всіх аспектів бізнесу, не лише безпосередньо пов'язаних із ІТ, а й обслуговування ключових бізнес-функцій та подальше відновлення – в тому числі, за потреби, голосових телекомунікацій, рівнів персоналу та фізичних об'єктів.

Останнім напрямком діяльності є відновлення нормальної роботи постраждалих інформаційних систем, сервісів та/або мережі. Відновлення ураженої системи (систем), служби (служб) та/або мережі (мереж) до безпечного робочого стану може бути досягнуто шляхом застосування виправлень для відомих вразливостей або вимкнення елемента, який був предметом компромісу. Якщо весь масштаб інциденту інформаційної безпеки

невідомий через знищення журналів під час інциденту, може знадобитися повна перебудова системи, служби та/або мережі [14].

10. Відповідь на кризові ситуації

Можлива ситуація, коли команда реагування на інциденти визначить, що інцидент інформаційної безпеки не контролюється і його необхідно перевести до кризової ситуації, використовуючи заздалегідь визначений план.

Найкращі варіанти боротьби з усіма можливими типами інцидентів інформаційної безпеки, які можуть вплинути на доступність і певною мірою цілісність інформаційної системи, повинні були бути визначені в плані антикризового управління організації. Ці параметри мають бути безпосередньо пов’язані з бізнес-пріоритетами організації та відповідними часовими рамками відновлення. Стратегія повинна передбачати наступне [14]:

- необхідні заходи попередження, стійкості та антикризового управління;
- необхідну організаційну структуру та відповідальність за реагування на кризову ситуацію;
- необхідну структуру та зміст плану або планів управління кризовою ситуацією.

План(и) кризового управління та засоби контролю, встановлені для підтримки активації цих планів(ів), після задовільної перевірки становлять основу для боротьби з більшістю ескалованих інцидентів, коли вони визначені критичними.

Залежно від типу інциденту та якщо він не контролюється, ескалація може призвести до серйозних заходів щодо подолання інциденту та активізації плану кризового управління, якщо такий є. Такі дії можуть включати, але не обмежуючись, активацію [14]:

- засобів пожежогасіння та процедури евакуації;
- засобів запобігання повеням та процедури евакуації;
- процесу деактивації вибухонебезпечних предметів та активацію відповідної процедури евакуації;

- підключення спеціалістів з розслідування шахрайства в інформаційній системі;
- підключення спеціалістів з розслідування технічних атак.

11. Логування активності і внесення змін

Важливо, що всі, хто бере участь у звітуванні та управлінні інцидентами інформаційної безпеки, повинні належним чином реєструвати всі дії для подальшого аналізу. Це повинно бути включено до форми звіту про інциденти інформаційної безпеки та в базу даних подій/інцидентів/вразливостей інформаційної безпеки, яка постійно оновлюється протягом циклу інциденту інформаційної безпеки від першого звіту до завершення перевірки після інциденту.

Цю інформацію слід зберігати в надійності та в належному режимі резервного копіювання. Крім того, усі зміни, внесені в контексті відстеження інциденту інформаційної безпеки і оновлення форми звіту про інциденти інформаційної безпеки та бази даних подій/інцидентів/вразливостей інформаційної безпеки, мають здійснюватися відповідно до офіційно прийнятої схеми контролю змін [14].

1.3.2. Процес управління інцидентами інформаційної безпеки відповідно до стандарту NIST SP 800-61

Відповідно до рекомендацій, NIST SP 800-61, ключових рекомендацій щодо забезпечення можливості організації реагувати на інциденти такі [15]:

- Встановіть формальні вимоги щодо реагування на інциденти.
- Створіть політику реагування на інциденти.
- Розробіть план реагування на інциденти на основі політики.
- Розробіть процедури реагування на інциденти.
- Встановіть політики та процедури взаємодії та обміну інформацією щодо інцидентів із зовнішніми сторонами.

- Надайте відповідну інформацію про інциденти відповідним організаціям.
- Визначте модель команди реагування на інциденти з урахуванням описаних вище факторів.
- Підберіть у команду реагування на інциденти співробітників з підходящою кваліфікацією.
- Визначте інші групи у межах організації, участь яких може знадобитися при обробці інциденту.
- Визначте, які послуги надаватиме команда з реагування на інциденти.

Згідно з даним стандартом, процес реагування на інциденти включає наступні фази: підготовка, виявлення та аналіз, стримування / усунення / відновлення, діяльність після інциденту (Рис. 1.3.2):

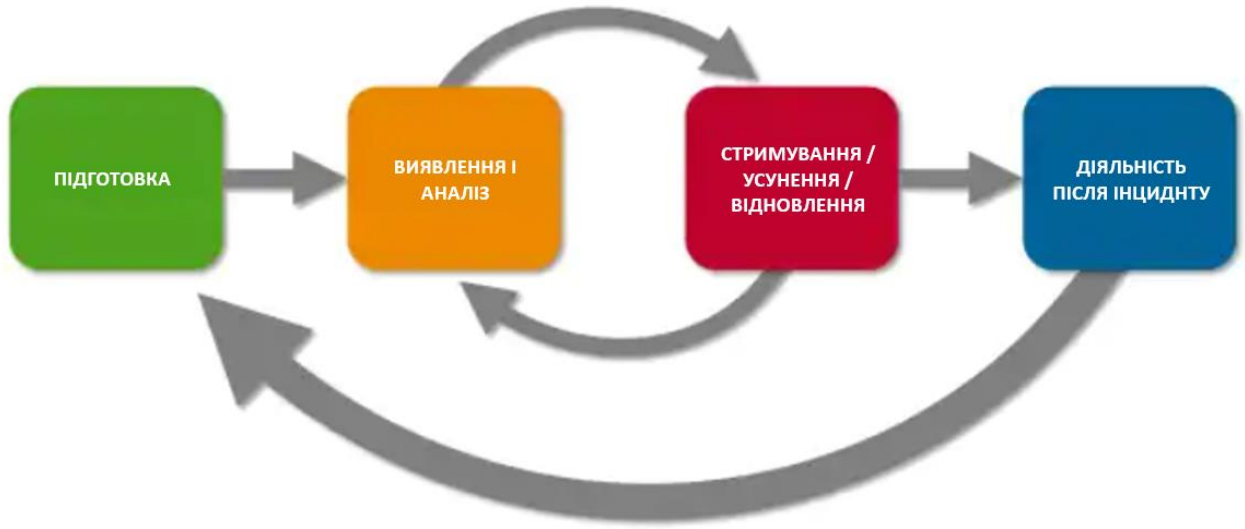

Рис. 1.3.2. Процес управління інцидентами інформаційної безпеки згідно з NIST SP 800-61 [15]

Даний стандарт наводить «чек-ліст» реагування на інциденти інформаційної безпеки [15]:

Фаза «Виявлення та аналіз»:

1) Визначити, чи відбувся інцидент.

a. Провести аналіз причин (передумов) та індикаторів.
b. Провести пошук інформації для кореляції.
c. Провести дослідження з використанням різних пошукових систем та баз знань.
d. Як тільки обробник переконається в наявності інциденту – почати документувати розслідування та збирання доказів.

2) Приорітезувати інцидент.

3) Повідомити про інцидент відповідним внутрішнім та зовнішнім сторонам.

Фаза «Стримування, усунення та відновлення»:

4) Виявляти, зберігати, захищати та документувати докази.

5) Локалізувати інцидент.

6) Усунути інцидент.

a. Виявити та усунути всі вразливості, які були використані.
b. Видалити шкідливе програмне забезпечення та інші небажані матеріали та компоненти.
c. У разі виявлення інших постраждалих систем (хостів), повторити кроки виявлення та аналізу, щоб виявити інших постраждалих, потім провести для них локалізацію та усунення інциденту.

7) Відновлення після інциденту.

a. Повернути системи у стан готовності до функціонування.
b. Переконатись, що системи функціонують належним чином.
c. За потреби здійснити додатковий моніторинг систем для виявлення відхилень від «нормального» функціонування.

Фаза «Діяльність після інциденту»:

8) Зробіть звіт щодо інциденту.

9) Проведіть зустріч для визначення засобів вдосконалення плану реагування (для великих інцидентів - обов'язково, для інших - опціонально).

Висновки до розділу 1

Отже, побудова ефективного процесу реагування на інциденти інформаційної безпеки ускладнена такими факторами як величезна кількість різноманітних загроз, яким неможливо запобігти зі стовідсотковою імовірністю, необхідність швидкого реагування, адже кожна хвилина затримки може призвести до непоправних збитків, необхідність грамотної побудови власне процесу реагування з урахуванням доступних ресурсів, мінімізація впливу людського фактору в ході процесу реагування для уникнення випадкових помилок.

Основні можливості вирішення проблем на шляху побудови процесу реагування - це дотримання рекомендацій загальноприйнятих стандартів, вивчення ефективних методик побудови даного процесу і їх адаптування під потреби організації, урахування актуальних для організації загроз і пріоритизація реагування на найбільш актуальні і небезпечні загрози, а також залучення ефективних засобів реагування на інциденти інформаційної безпеки.

Проблематика побудови процесу реагування на інциденти інформаційної безпеки була неодноразово досліджена провідними спеціалістами, тому при побудові даного процесу в організації доцільно дотримуватись рекомендацій міжнародно визнаних стандартів інформаційної безпеки.

І навіть при дотриманні всіх стандартів для забезпечення миттєвого виявлення і реагування на інциденти важливою складовою правильно побудованого процесу реагування на інциденти є автоматизація.

Розділ 2

АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПОБУДОВИ АВТОМАТИЗОВАНИХ СЦЕНАРІЇВ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1. Інструменти автоматизації реагування на інциденти інформаційної безпеки

2.1.1. Автоматизація в життєвому циклі обробки інциденту

Як було зазначено в минулому розділі, для досягнення найвищої ефективності і надійності, процес реагування на інциденти інформаційної безпеки має бути максимально автоматизований.

Для виконання автоматичних дій і для більшості інших не організаційних задач – ефективного виявлення, аналізу і обробки зловмисних дій, використовуються рішення інформаційної безпеки. Під рішеннями (або продуктами) інформаційної безпеки розуміються технологічні інструменти та послуги, програмне або апаратне забезпечення, яке допомагає захистити організації від кібератак [16].

Універсальний керований план виявлення та реагування є найкращим способом вирішення задачі обробки інцидентів [6]. І фактично кожен крок побудови даного процесу включає використання тих чи інших рішень інформаційної безпеки.

Загалом існує п’ять етапів життєвого циклу управління інцидентами, визначених Бібліотекою IT-інфраструктури (Information Technology Infrastructure Library - ITIL):

1) Ідентифікація
2) Логування
3) Категоризація
4) Розстановка пріоритетів

5) Реагування

Рекомендований процес ITIL акцентує увагу на тому, що більша частина процесу реагування – це планування. Перші чотири пункти присвячені підготовчій роботі, заключний являє собою активну реакцію.

Однак сучасні прогресивні та ефективні комплексні рішення для виявлення і реагування на інциденти інформаційної безпеки слідують скороченому процесу, що включає чотири ключові області. Це передбачає об'єднання ідентифікації, логування, категоризацію та пріоритезацію в одну початкову процедуру виявлення загроз. Наступні кроки спрямовані на негайну відповідь, подальший аналіз і керування виправленнями [6].

1. Виявлення загроз

Найширшою сферою управління інцидентами є виявлення. Дуже важливою задачею є створення надійних наборів даних, каталогізація всіх відповідних ресурсів, які можуть бути скомпрометовані (або використані) під час інциденту. Якщо організація не має належного доступу до інформації, першим кроком є процес збору та оптимізації її для побудови подальшого процесу.

Якщо дані існують, виявлення починається з регулярного моніторингу та оновлення цих даних. Виявлення — це не одноразовий аналіз, а безперервний процес.

Щоб виявити загрози, вкрай важливо встановити базовий рівень того, як виглядає система за відсутності поточних інцидентів. Щойно цей базовий рівень буде встановлено, можна легко помітити та негайно класифікувати загрозу і почати процес реагування на неї, щойно вона з'явиться.

2. Реагування на інцидент

Коли загрози виявлено, класифіковано та впорядковано за пріоритетністю, формується план боротьби з ними. Потім йде фаза відповіді.

Фаза реагування складається з двох рівнів або форм реагування:

1) Негайна реакція – будь-яка екстрена тактика, необхідна для зупинення прогресу зловмисника та запобігання подальшій шкоді. Це може

включати зміни або навіть повну зупинку певних процедур, від яких залежить бізнес.

2) Довгострокове відновлення – включає процеси відновлення скомпрометованих активів, усунення вразливостей і встановлення превентивних заходів, щоб запобігти подібним інцидентам у майбутньому.

Інцидент може або не може змусити організацію призупинити деякі або всі звичайні процедури. У випадках, коли дії були призупинені, потрібно буде завершити принаймні негайну відповідь, перш ніж повернутися до нормального режиму.

3. Аналіз причин

Цю область можна вважати частиною довгострокового процесу відновлення, згаданого вище.

Аналіз причин передбачає поглиблений аналіз інфраструктури кібербезпеки організації та історію конкретної атаки, щоб визначити, як це сталося. Зловмисники часто користуються вразливими місцями, які не були відомі компанії на момент атаки. Розуміння глибини та ширини власного (не)розуміння є ключовим для усунення якомога більшої кількості таких невідомих слабких місць.

Тестування на проникнення, також відоме як пентест, є формою етичного хакерства, яка допомагає організації зрозуміти, що зробив би хакер, якби атакував вас. Симулюючи атаку та уважно вивчаючи рухи хакера, можна краще підготуватись до майбутніх атак.

4. Відповідність нормативним вимогам

Інколи відповідність нормативним вимогам передбачає деякі з найбільших проблем у виявленні інцидентів і реагуванні на них. Однак зворотна сторона цього рівняння полягає в тому, що організації, які дотримуються і перевищують інструкції щодо відповідності, добре підготовлені до управління інцидентами.

Якщо в організації немає впевненості, які саме елементи необхідні для досягнення повної відповідності, аналітичні інструменти, як-от звіт про доступність виправлень, можуть визначити різноманітне обладнання, програмне забезпечення та методи, які необхідно застосувати. Це стосується всіх інструкцій, включаючи, але не обмежуючись:

- PCI-DSS і ASV для всіх компаній, що обробляють кредитні картки
- HIPAA та HITECH для всіх компаній, які працюють з медичними документами
- CMMC / NERC CIP для підрядників з Міністерством оборони або критичною енергетичною інфраструктурою

Комплексні консультаційні послуги щодо відповідності можуть допомогти організації досягти оптимального управління інцидентами, а також загальної точності кібербезпеки.

Отже, майже для всіх кроків типової, рекомендованої послідовності обробки інцидентів необхідні інструменти інформаційної безпеки, які являють собою ресурсне забезпечення процесу реагування. А також важливим фактором є забезпечення централізованої платформи обробки інцидентів, в якій може бути зібрана вся необхідна інформація і автоматично виконані дії миттєвого реагування.

2.1.2. Інструменти автоматизації процесу реагування на інциденти

Існує кілька типів інструментів, які можливо використати для централізації процесу реагування на інциденти інформаційної безпеки [17]:

1. Оркестровка безпеки, автоматизація та реагування (Security Orchestration, Automation and Response - SOAR)

SOAR відноситься до платформ, які пропонують інструменти для збору даних безпеки з різних джерел. Рішення SOAR може поєднувати машинне навчання та ручний аналіз для отримання даних, аналізу і визначення пріоритетів відповідних процедур реагування на інциденти.

Програмне забезпечення SOAR зазвичай включає основні три можливості:

1) Централізація даних

2) Реагування на інциденти

3) Автоматизація операцій безпеки

Організації використовують SOAR для інтеграції з різноманітними джерелами, що забезпечує автоматичне реагування на загрози.

2. Аналітика поведінки користувачів і суб'єктів (User and Entities Behavior Analysis - UEBA)

Рішення UEBA використовують великі набори даних і машинне навчання для встановлення базових показників для типових моделей поведінки, що дозволяє їм ідентифікувати нетипову поведінку в мережі, яка може вказувати на загрози. Акцент на підозрілій поведінці дозволяє UEBA виявляти загрози, які можуть оминути традиційні інструменти безпеки та антивірусні засоби, включно з атаками, не заснованими на зловмисному програмному забезпеченні.

UEBA використовує поведінкові моделі для оцінки рівнів загрози, надаючи оцінки ризику, щоб керувати процесом реагування.

3. Інформація про безпеку та керування подіями (Security Information and Event Management - SIEM)

SIEM — це підхід до управління безпекою, який забезпечує уніфіковану систему для поєднання функцій керування інформацією та подіями. Рішення SIEM розгортають кілька агентів збору даних для ієрархічного збору даних про події із серверів, пристроїв кінцевих користувачів та мережевої інфраструктури. Центральна консоль керування консолідує дані, дозволяючи аналітикам безпеки фільтрувати шум і визначати пріоритетність реальних інцидентів безпеки.

4. Виявлення і реагування на загрози на кінцевих точках (Endpoint Detection and Response - EDR)

Системи EDR збирають і аналізують дані безпеки кінцевих точок, щоб захистити мережу від вразливих пристроїв і робочих станцій користувачів. EDR

спрямований на виявлення порушень безпеки в режимі реального часу, що забезпечує швидке реагування. Цей підхід допомагає ідентифікувати нові та прогресивні загрози, які традиційні засоби безпеки можуть не використовувати. Конкретні можливості кожного рішення EDR можуть значно відрізнятися.

5. Розширене виявлення та реагування на загрози (Extended Detection and Response - XDR)

Рішення XDR — це інструменти для виявлення загроз безпеці та впровадження процедур реагування на інциденти. Інструменти XDR об’єднують кілька можливостей безпеки в уніфіковане рішення для операцій безпеки, що робить складні можливості реагування на інциденти більш доступними.

Перевагою XDR є консолідація кількох продуктів безпеки, що базуються на можливостях EDR. Він може підвищити продуктивність операцій безпеки завдяки вдосконаленому виявленню та реагування, а також централізованій видимості та контролю в корпоративному середовищі. Інструменти XDR приймають і дистилюють кілька телеметричних потоків і аналізують вектори загроз і тактику. Вони допомагають прискорити реагування, керуючи процесами виявлення та розслідування.

Кожне з цих рішень може принести користь при побудові процесу реагування на інциденти на кінцевих точках, проте найбільш ефективним з точки зору централізації всієї наявної інформації і забезпечення максимальної автоматизації процесу реагування є рішення SOAR. Варто зазначити, що SOAR самостійно не збирає жодних даних та не виконує жодних дій. Це виключно платформа, яка забезпечує інтеграцію інших рішень в одній консолі і надає необхідний для розслідування інцидентів функціонал.

2.2. Опис методики, послідовності розробки сценаріїв реагування на інциденти інформаційної безпеки

Реалізація будь-яких процесів, що повинні бути реалізовані в організації, неможлива без достатнього ресурсного забезпечення [18]. Для побудови процесу реагування на інциденти в першу чергу необхідно виділити достатню кількість ресурсів – працівників, що будуть займатись розробкою сценаріїв реагування, фінансування закупки і підтримки відповідних рішень інформаційної безпеки, відповідно час на реалізацію задачі, а також ресурси для постійного моніторингу стану автоматизованої системи реагування.

1) Першим кроком у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація класів інцидентів [18].

Переважно всюди для попередньої класифікації класів інцидентів фактично використовуються рішення інформаційної безпеки для виявлення і реагування на загрози різних типів – такі як рішення забезпечення антивірусного захисту (Next Generation Antivirus - NGAV, EDR), міжмережеві екрани (Intrusion Detection System - IDS, Intrusion Prevention System IPS), контроль безпеки хмарних ресурсів, захист корпоративної пошти тощо.

Також в подібних рішеннях майже завжди для класифікації інцидентів використовується фреймворк MITRE ATT&CK [19], або Cybersecurity Kill Chain [20]. Це дозволяє забезпечити уніфікацію типів інцидентів інформаційної безпеки організації, що надходять з різних рішень та забезпечує відповідність міжнародним нормам класифікації інцидентів.

2) Другим кроком є розробка сценаріїв реагування для кожного актуального в організації типу інциденту з урахуванням доступних або запланованих для придбання засобів.

Загалом процес систематизації і автоматизації процесу реагування на інциденти інформаційної безпеки є непростим і доволі довгим. Тому найчастіше на початкових етапах впровадження автоматизації обирають декілька найбільш актуальних типів інцидентів і першочергово розробляють

для них ефективні сценарії реагування та автоматизують кроки, які можливо виконати без залучення аналітика інформаційної безпеки.

При розробці сценарію в першу чергу необхідно враховувати вхідні дані (які є можливості для виявлення інциденту і яка інформація доступна на початку розслідування) і бажаний результат, часові рамки розслідування. Для ефективної побудови автоматизації процесу реагування на інциденти, сценарії для обраних типів інцидентів обов'язково мають бути задокументовані в тому чи іншому вигляді з чітким описом послідовності дій, позначенням автоматизованих етапів і моментів, в яких має бути прийняте рішення про подальші дії аналітиком інформаційної безпеки. Сценарії можуть бути задокументовані в графічному вигляді (блок-схема) або у вигляді послідовних пунктів.

3) Третім кроком є власне автоматизація розроблених сценаріїв з використанням відповідних рішень інформаційної безпеки. В результаті для побудови зручного і ефективного, автоматизованого процесу реагування в організації необхідні інструменти для збору даних (з кінцевих точок, мережевих пристроїв, поштових серверів, серверів управління доменом, хмарних активів тощо), бажано інструмент для централізації і кореляції даних (клас рішень SIEM) і власне для автоматизації необхідне рішення класу SOAR.

Даний крок полягає в тому, щоб реалізувати розроблені сценарії реагування у відповідних рішеннях – налаштувати збір даних, забезпечити можливість виявлення інцидентів, централізацію інформації з різних джерел, підключення необхідних рішень до системи SOAR за допомогою інтеграцій, і власне налаштування сценаріїв у самій системі SOAR.

2.3. Опис тестового середовища

Для подальшого наведення прикладів розроблених сценаріїв реагування необхідно визначити і описати тестове середовище, як було зазначено раніше, - рішення інформаційної безпеки які доступні в організації-прикладі.

Розробка сценаріїв реагування з використанням рішення SOAR є скоріше привілеєм великих організацій з достатнім бюджетуванням інформаційної безпеки і з можливістю створення різних підрозділів в рамках роботи спеціалістів інформаційної безпеки.

Тому для подальшої розробки прикладів сценаріїв реагування з використанням рішення SOAR на основу буде взято організацію з достатнім ресурсним забезпеченням інформаційної безпеки і впровадженими функціонуючими різноманітними рішеннями інформаційної безпеки, які можуть бути інтегровані в SOAR.

Для розробки сценаріїв не є важливою прив’язка до конкретних вендорів, тому за основу буде взято класи рішень, більшість із яких зможе забезпечити описаний в подальшому функціонал.

Отже, використовуваний в тестовому середовищі набір рішень включає:

- SOAR, для централізації і автоматизації процесу реагування на інциденти інформаційної безпеки
- SIEM, для збору і кореляції даних, які в ряді сценаріїв можуть бути використані як вхідні дані для генерації інциденту в SOAR
- Endpoint Protection (EPP), для збору даних і реагування на загрози на кінцевих точках
- Data Loss Prevention (DLP), для контролю за витоком конфіденційних даних
- Lightweight Directory Access Protocol (LDAP), для управління користувачами
- Threat Intelligence (TI), для отримання важливих даних про загрози в рамках організації
- Service Desk, для ще більш зручної організації роботи співробітників безпеки
- Messaging Gateway, для перевірки і фільтрації вхідних електронних листів
- Email Security Appliance (ESA), для додаткової перевірки безпеки пошти.

Ситуація в організації на момент перегляду процесу реагування на інциденти інформаційної безпеки – наведені рішення, окрім SOAR, впроваджені і функціонують, використовуються при обробці інцидентів.

Наявні в організації проблеми:

- Процес реагування на інциденти інформаційної безпеки недостатньо структурований і організований, інструкції недостатньо деталізовані і не задокументовані
- У нових співробітників йде багато часу на розуміння типового процесу обробки інцидентів різних типів
- При аналізі інциденту аналітик має переключатись між консолями різних рішень для отримання необхідної інформації або виконання дій і зіставляти дані з різних рішень вручну
- Звітування по виконаним для обробки інциденту діям не структуроване, некоректно задокументоване або відсутнє
- Можливість звітування по загальній ситуації оброблених інцидентів
- Недостатній рівень комунікації співробітників організації в рамках процесу реагування на інциденти інформаційної безпеки

Для виправлення зазначених проблем в організації виділено бюджет на придбання, впровадження і підтримку рішення SOAR.

Варто зазначити, що SOAR в недостатньо зрілих компаніях в плані організації інформаційної безпеки часто перетворюється на автоматизацію заради автоматизації. Тому плануванням сценаріїв реагування має займатись кваліфікований в управлінні інформаційною безпекою спеціаліст.

Перед тим як впроваджувати рішення SOAR, в компанії і ідеалі мають бути вже розроблені і задокументовані сценарії реагування на різні типи інцидентів, які покладаються на вже наявні рішення.

При недостатньому рівні розуміння функціоналу SOAR, при використанні неправильного підходу до його налаштування, дане рішення ніяк не зможе допомогти в управлінні інцидентами інформаційної безпеки.

Саме тому в даній роботі далі наведено приклади послідовності розробки і впровадження сценаріїв реагування на декілька найбільш розповсюджених типів інцидентів.

Висновки до розділу 2

В даному розділі визначено, що ефективний процес реагування на інциденти інформаційної безпеки в умовах сьогодення може бути створений виключно з використанням відповідних якісних рішень інформаційної безпеки.

Важливо надати ресурсне і організаційне забезпечення на кожному етапі обробки інциденту – загальновизнані методи збору інформації з максимальним рівнем видимості і інструменти аналізу інформації, що використовують прогресивні методи аналізу даних, а також визначення відповідальних за процес реагування на інциденти інформаційної безпеки осіб.

Розглянуто коректну послідовність дій і необхідну попередню аналітичну роботу для розробки ефективного сценарію реагування на інцидент інформаційної безпеки.

Для подальшої розробки прикладів сценаріїв реагування на визначені типи інцидентів інформаційної безпеки, наведено вхідні дані тестового середовища – наявні рішення інформаційної безпеки і проблеми організації реагування на інциденти, які мають бути вирішені з впровадженням розроблених за наведеним далі принципом автоматизованих сценаріїв реагування на інциденти інформаційної безпеки.

Розділ 3

РОЗРОБКА ТА ЗАСТОСУВАННЯ СЦЕНАРІЇВ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

3.1. Сценарій реагування на інциденти типу "Фішинг"

3.1.1. Опис процесу планування сценарію реагування на інциденти типу "Фішинг"

Перший крок побудови сценарію реагування визначено, тип інциденту – фішинг. Другий крок – необхідно зрозуміти вхідні дані – звідки і в якому вигляді надходить інформація про виявлення загрози типу «фішинг» і якого результату необхідно досягти. В даному випадку необхідно досягти уникнення або принаймні мінімізації збитків від даної загрози, при цьому забезпечивши співробітникам доступ до інформації, якщо спрацювання є помилковим. Тобто основною метою процесу реагування є визначення чи дійсно фішинговий лист є небезпечним і містить загрозу для інформаційної безпеки організації, чи він є санкціонований і має надійти користувачу для уникнення порушення бізнес-процесів.

Ризик від помилкового допуску зловмисного листа до користувача є значним, тому не можна пропустити підозрілий лист до того, як буде визначено, що він є безпечним. При цьому не можна значно затримувати надходження листа (якщо він безпечний), адже це може спричинити порушення бізнес-процесів.

Аналіз всіх листів, що надходять в організацію, перед їх пропуском є вкрай часо- і ресурсовитратним, невиправданим процесом. Тому на даному етапі необхідно додати елемент автоматизації. Для цього враховуючи початкові умови, наявні в організації інструменти, можна використати рішення класу захисту корпоративної пошти – Messaging Gateway.

Messaging Gateway аналізуватиме вхідну пошту відповідно до попередньо заданих налаштувань і пропускатиме санкціоновані листи, затримуючи підозрілі. Сповіщення від Messaging Gateway про затриманий підозрілий лист в даному випадку і будуть вхідними даними для генерації інциденту і ініціації сценарію розслідування.

При подібному блокуванні листа існує імовірність помилкового спрацювання (false positive), тому необхідно проводити аналіз заблокованих листів. Для цього можна проаналізувати вміст листа – текст, вкладення, наявні в листі дані, що можна класифікувати як артефакти (хеші, IP-адреси, доменні імена). Для аналізу цих визначених даних можна використати платформи / інструменти (бази даних) артефактів. В даному випадку можна використати корпоративне рішення Threat Intelligence для аналізу артефактів. І у випадку, якщо жоден з артефактів не визначений як зловмисний, можна додатково запустити перевірку листа (в першу чергу посилань і прикріплених файлів) в пісочниці з використанням рішення класу Email Security Appliance (далі – ESA).

Також при розробці сценарію реагування важливо враховувати, що цей процес необхідно постійно аналізувати і покращувати для забезпечення оптимізації. І якщо є механізм, який дозволить статично відсікати, наприклад, точно небезпечні листи, бажано його реалізувати. Наприклад, в даній типовій організації всі дані централізовано зберігаються в SIEM рішенні. Там також наявний механізм фільтрації листів електронної пошти, що надходять в організацію. Тому при виявленні небезпечних листів, можна додавати їх артефакти відповідно в списки блокування SIEM, і наступного разу аналогічний лист не надійде на вхід ESA і не потребуватиме повторного аналізу.

Звичайно якщо заблокований лист при аналізі визначений безпечним – його необхідно в незмінному вигляді надіслати користувачу.

Так може виглядати текстовий опис приблизно розпланованого сценарію реагування на інцидент інформаційної безпеки типу «фішинг» з урахуванням наявних в компанії інструментів – рішень інформаційної безпеки, що можуть допомогти в розслідування даного типу інциденту. Звичайно від початкової ідеї

до кінцевого результату, який вирішено реалізовувати в організації і сценарії реагування можуть вноситись масштабні зміни. Кінцева реалізація може повністю відрізнятись від текстового опису, плану, або розробленої блок-схеми, якщо наприклад у адміністратора безпеки, що займався його розробкою, відсутній досвід роботи з рішенням SOAR (або з іншими задіяними рішеннями) і розуміння принципів їх роботи. Важливий момент - саме кінцева реалізація обов’язково має бути задокументована і описана, в ідеалі збережена як остання версія сценарію і прописана в офіційній документації організації (наприклад як документ-інструкція).

Автоматизація кроків сценарію також визначається за деякими факторами. Всі процеси передачі інформації з одного рішення в інше бажано автоматизувати, якщо це можливо, для збереження часу аналітика. Адже при передачі інформації не приймаються безпосередні рішення і не вимагається аналіз даних. Для інших моментів сценарію, в перу чергу, необхідно зрозуміти чи може рішення на цьому етапі бути прийняте автоматично, чи є в організації достатньо засобів, які вичерпно і коректно визначать наступний крок. Наприклад, для досліджуваного плейбуку це може бути аналіз артефактів в Threat Intelligence рішенні, адже аналітик не виконає пошук і аналіз краще, ніж відповідна програма, рішення, затверджене для використання в організації.

На початкових етапах використання автоматизованого сценарію реагування можна додати ручні завдання для перевірки коректності виконання етапу, а в подальшому прибрати їх або приховати. Для деяких задач можна залишити як автоматизоване рішення, так і ручне підтвердження коректності прийнятого рішення аналітиком.

Звичайно для цих випадків необхідно також оцінити можливість і трудомісткість відповідної автоматизації. В рідкісних випадках написання інтеграцій для автоматизації є вкрай складним або неможливим. Також на початковому етапі можливо прийняття рішення про ручну обробку певного етапу і запланувати його автоматизацію в подальшому.

І другий тип рішень в сценарії реагування – коли в організації недостатньо засобів автоматизованого аналізу (або достатньо надійних рішень для даної задачі не існує) і рішення обов’язково має приймати аналітик. Подібні задачі можуть як бути, так і не бути наявні в сценарії, залежно від типу інциденту і задачі реагування.

Планування сценарію загалом може відбуватись по різному, залежно від адміністратора, який цим займається. Наприклад, можна зробити це в декілька етапів:

- визначити пріоритетний для автоматизації тип інциденту;

- розписати приблизну послідовність дій, яка необхідна для розслідування інциденту і варіанти кінцевого результату;

- детально розписати послідовність дій, дії при різних результатах виконання умов сценарію

- побудувати блок-схему дій, при наявності досвіду роботи з рішенням SOAR можна одразу враховувати формат сценарію в системі;

- перенести сценарій в систему SOAR, забезпечити необхідні інтеграції і налаштування, протестувати і відредагувати за необхідністю;

- відповідно відредагувати схему, опис сценарію та затвердити документально.

Після виконання всіх попередніх дій можна вводити автоматизований сценарій реагування на інцидент відповідного типу в експлуатацію в організації.

Деякі організаційні моменти, як наприклад визначення працівників, що відповідатимуть за контроль системи SOAR, виконання ручних етапів розслідування, налаштування інструментів безпеки не розглянуто в даній статті.

3.1.2. Текстовий опис сценарію

В результаті, перший приблизний план може мати такий вигляд:

Проект сценарію обробки подій для виявлення фішингу:

1. Електронні листи на вхід SOAR надходять з Messaging Gateway (якщо їх визначено як підозрілі), або лист надходить від адміністратора безпеки.

2. SOAR виконує розбір листа, виділяє, якщо там є лінкі, вкладення, створює інцидент, додає в артефакти вкладення, лінкі, IP-адресу відправника, причину карантину.

3. Отримуємо (вираховуємо) хеш на вкладення, яке дістали з листа.

4. Через API звертаємось до репозиторію зразків коду Threat Intelligence та шукаємо там хеш вкладення, лінкі, IP-адресу.

a. Якщо в TI знаходимо, то по API звертаємось до SIEM та перевіряємо що там є ці IP-адреса, лінки. Якщо їх там немає то додаємо.

b. Якщо в TI не знаходимо то ідемо на Virus Total (VT) \ IBM xForce (загальнодоступні джерела даних про загрози) та шукаємо там хеш, лінкі, IP-адреси. Якщо є негативна інформація щодо цих артефактів то по API заносимо в корпоративне сховище Threat Intelligence вкладення, IP-адресу відправника, лінкі.

i. Якщо на VT\IBM xForce не знаходимо нічого негативного по хешам, лінкам, IP-адресам, необхідно закрити інцидент та відправити оригінал листа на ESA для аналізу.

ii. Якщо від ESA прийде інформація, що там нічого не виявлено підозрілого чи зловмисного, ESA повідомляє інформацію про статус розгляду листа в SOAR та відправляє лист отримувачу.

iii. Якщо від ESA прийде інформація, що у листі виявлено підозрілі вкладення чи зловмисний код, лист блокується в карантині ESA, ESA повідомляє інформацію про статус розгляду листа в SOAR, по API звертаємось до SIEM та перевіряємо що там є ці IP-адреса, лінки. Якщо їх там немає то додаємо. Закриваємо інцидент.

На основі початкового плану можна розробити детальну послідовність дій з урахуванням логіки роботи системи і інтеграцій:

1) На вхід SOAR надходить лист з MG, з якого генерується інцидент. За допомогою скрипту лист оброблюється і необхідні дані – посилання, IP-адреси, причина карантину зберігаються в системі.

2) За допомогою кастомної інтеграції обробляється вкладення за наявності – вираховується хеш файлу. Якщо файл – архів формату zip – вираховується хеш усіх вкладених файлів.

3) Здійснюється перевірка наявності значень артефактів в TI, артефакти поділяються на 2 списки – наявні в TI (1), відсутні в TI (2).

4) Для списку (2) перевіряється наявність спрацювань в підключених загальнодоступних джерелах даних про загрози. Проаналізовані артефакти поділяються на 2 списки – наявні спрацювання (3), відсутні спрацювання (4).

Умова: дані відсутні в списку (3):

5) Перевіряється наявність даних зі списку (2) в SIEM та вносяться відсутні дані.

6) Закривається інцидент

Умова: дані наявні в списку (3):

5) Надсилається оригінал листа на ESA.

6) Здійснюється ручна перевірка результату (виконується видане завдання), відмічається відповідний результат згідно з інструкціями.

Умова: лист безпечний.

7) Вносяться артефакти зі списку (3) в TI.

8) Перевіряється наявність даних зі списку (2) і списку (3) в SIEM та вносяться відсутні дані.

9) Закривається інцидент.

Умова: лист зловмисний.

7) Вносяться артефакти зі списку (3) і списку (4) в TI.

8) Перевіряється наявність даних зі списку (2), списку (3) і списку (4) в SIEM та вносяться відсутні дані.

9) Закривається інцидент.

3.1.3. Графічний опис і реалізація сценарію

І відповідно до детального опису подій можна розробити блок-схему для візуалізації дій сценарію реагування (Рис.3.1.1):

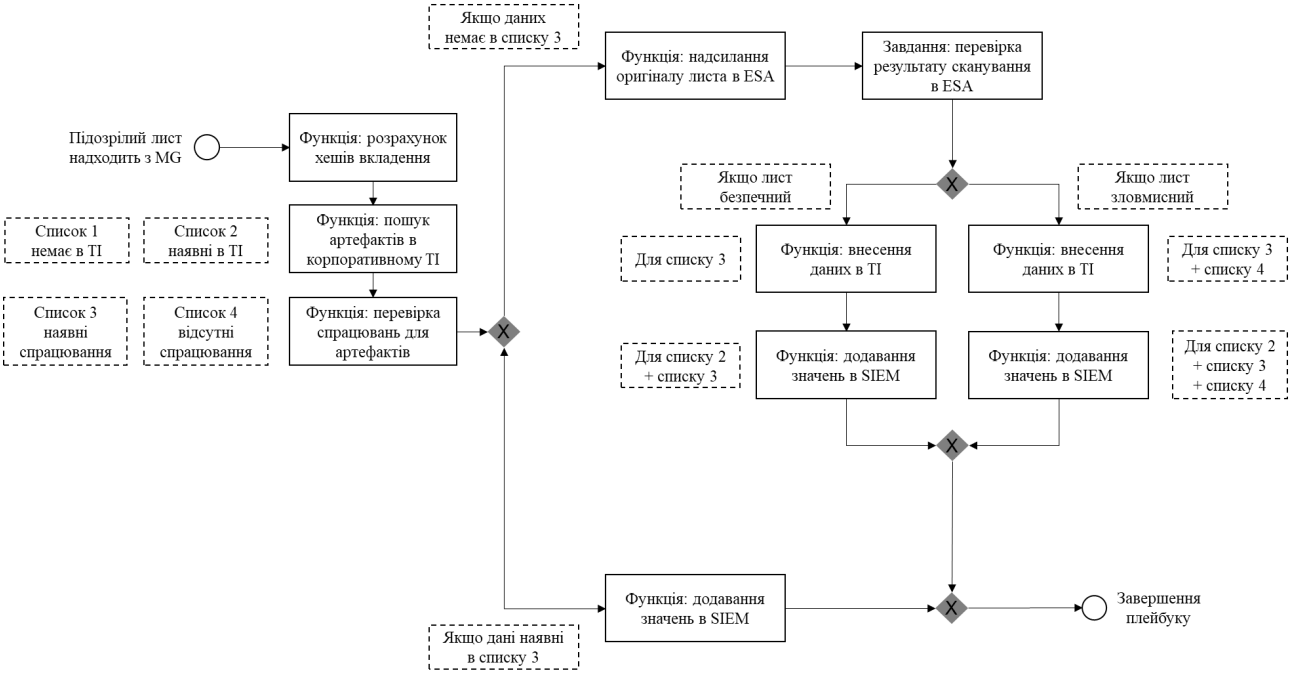

Рис. 3.1.1. Блок-схема сценарію реагування на інцидент типу «Фішинг» (розробка автора)

Дану блок-схему також наведено в Додатку А (Рис. А.1) для більш зручного перегляду.

3.2. Сценарій реагування на інциденти типу "Зловмисне програмне забезпечення"

3.2.1. Опис процесу планування сценарію реагування на інциденти типу "Зловмисне програмне забезпечення"

Вхідними даними для розслідування інциденту типу «Зловмисне програмне забезпечення» в даному тестовому середовищі буде спрацювання рішення EPP. Загалом рішення EPP може бути достатньо для обробки інцидентів подібного типу і часто від SOAR вимагається тільки організація роботи аналітиків.

Проте в даному тестовому середовищі розглянуто необхідність збагачення корпоративного TI артефактами, пов’язаними зі спрацюванням і додаткове сповіщення адміністраторів різних рішень інформаційної безпеки про результати обробки інциденту.

Тому після генерації інциденту в SOAR має бути проведено аналіз наявних індикаторів – хешу файлу, IP-адрес підключень тощо, перевірено їх на фактор зловмисного впливу і при підтвердженні додано у інші необхідні рішення інформаційної безпеки для фільтрації подібних випадків до потрапляння на кінцеві точки.

Таким чином досягається скорочення кількості інцидентів, що генеруються в рішенні EPP і відповідно кількість повторюваних одноманітних інцидентів.

В даному плейбуці якщо функціональні можливості конкретних використовуваних рішень інформаційної безпеки це дозволяють, можуть бути автоматизовані всі кроки обробки інциденту.

3.2.2. Текстовий опис сценарію

Перший приблизний план сценарію може мати такий вигляд:

1. Відслідковуємо події що фіксуються в рішенні EPP про знайдені вірусні файли або підозрілі файли (наявна інформація про такі події вміщує в себе ім’я такого файлу, хост, де його знайдено, шлях у файловій системі, його хеш та інше).
2. Через API звертаємось до репозиторію зразків коду TI та шукаємо там хеш вкладення, лінкі, IP-адресу.
    1. Якщо в TI знаходимо, по API звертаємось до SIEM та перевіряємо що там є ці IP-адреса, лінки щодо цього файлу. Якщо їх там немає то додаємо, відправляємо адміністраторам SIEM листа про додавання інформації.

2. Якщо в TI не знаходимо то створюємо інцидент в SOAR, ідемо на VT \ IBM xForce та шукаємо там по хеш інформацію щодо цього файлу. Якщо є негативна інформація щодо цього файлу то по API, заносимо в TI вкладення (якщо є), IP-адресу control-центрів цього зловмисного коду, лінкі на сайти пов’язані з розповсюдженням цього файлу до SIEM для подальшого блокування цього трафіку. Направляємо адміністраторам SIEM лист про додавання інформації в SIEM. Надсилаємо адміністраторам відділу контролю лист про погану репутацію файлу.

3. Перевіряємо в SOAR чи були за останній день інциденти\події від хоста де знайдено вірус. Якщо так, то через API рішення EPP додаємо хост де знайдено вірус до групи на примусове сканування.

4. У виконаних діях щодо цього інциденту прописуємо усе що зробили, закриваємо інцидент.

5. Направляємо адміністраторам SIEM лист про додавання інформації. Адміністраторам EPP надсилаємо лист про погану репутацію файлу та про виконані дії щодо сканування.

На основі початкового плану можна розробити детальну послідовність дій з урахуванням логіки роботи системи і інтеграцій:

1) Дані на вхід SOAR отримуються з бази даних EPP рішення – записи про знайдені вірусні / підозрілі файли, значення з бази даних вносяться в поля SOAR.
2) Здійснюється перевірка наявності значень артефактів в корпоративному TI, артефакти поділяються на 2 списки – наявні в TI (1), відсутні в TI (2).
3) Для списку (2) перевіряється наявність спрацювань в підключених загальнодоступних джерелах даних про загрози. Проаналізовані артефакти поділяються на 2 списки – наявні спрацювання (3), відсутні спрацювання (4).
4) Вносяться артефакти зі списку (3) в TI.

5) Перевіряється наявність артефактів зі списку (1) і списку (3) в SIEM, формується список (5) – дані, відсутні в SIEM.
6) Вносяться артефакти зі списку (1) в SIEM.

Умова: список (5) містить дані.

7) Вносяться артефакти зі списку (5) в SIEM.

8) Надсилається лист адміністраторам SIEM про додавання даних.

Умова: список (3) містить дані.

9) Надсилається лист адміністраторам відділу контролю про погану репутацію файлу.

10) Виконується запит в SIEM на перевірку наявності спрацювань з даним хостом за останню добу.

Умова: спрацювання для даного хосту за останню добу наявні

11) Ініціюється примусове сканування задіяного хоста в EPP.

12) Перевіряються результати сканування в EPP.

13) Надсилається лист адміністраторам EPP про результати сканування.

14) Закривається інцидент

Умова: спрацювання для даного хосту за останню добу відсутні.

11) Закривається інцидент.

Умова: список (3) не містить дані.

9) Виконується запит в SIEM на перевірку наявності спрацювань з даним хостом за останню добу.

Умова: спрацювання для даного хосту за останню добу наявні

10) Ініціюється примусове сканування задіяного хоста в EPP.

11) Перевіряються результати сканування в EPP.

12) Надсилається лист адміністраторам EPP про результати сканування.

13) Закривається інцидент

Умова: спрацювання для даного хосту за останню добу відсутні.

10) Закривається інцидент.

Умова: список (5) не містить дані.

Умова: список (3) містить дані.

7) Надсилається лист адміністраторам групи контролю про погану репутацію файлу.

8) Виконується запит в SIEM на перевірку наявності спрацювань з даним хостом за останню добу.

Умова: спрацювання для даного хосту за останню добу наявні

9) Ініціюється примусове сканування задіяного хоста в EPP.

10) Перевіряються результати сканування в EPP.

11) Надсилається лист адміністраторам EPP про результати сканування.

12) Закривається інцидент

Умова: спрацювання для даного хосту за останню добу відсутні.

9) Закривається інцидент.

Умова: список (3) не містить дані.

7) Виконується запит в SIEM на перевірку наявності спрацювань з даним хостом за останню добу.

Умова: спрацювання для даного хосту за останню добу наявні

8) Ініціюється примусове сканування задіяного хоста в EPP.

9) Перевіряються результати сканування в EPP.

10) Надсилається лист адміністраторам EPP про результати сканування.

11) Закривається інцидент

Умова: спрацювання для даного хосту за останню добу відсутні.

8) Закривається інцидент.

3.2.3. Графічний опис і реалізація сценарію

І відповідно до детального опису подій можна розробити блок-схему для візуалізації дій сценарію реагування (Рис.3.2.1):

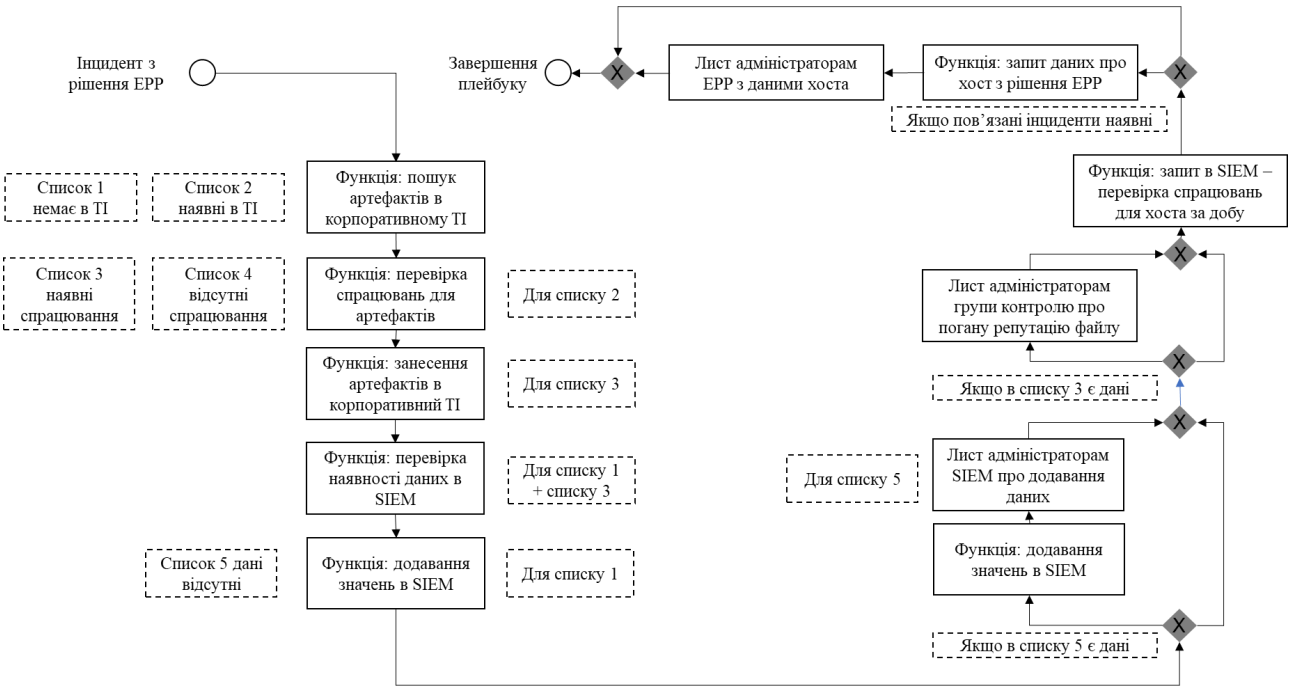

Рис. 3.2.1. Блок-схема сценарію реагування на інцидент типу «Зловмисне програмне забезпечення» (розробка автора)

Дану блок-схему також наведено в Додатку А (Рис. А.2) для більш зручного перегляду.

Висновки до розділу 3

В даному розділі наведено послідовність розробки двох сценаріїв реагування на типові інциденти інформаційної безпеки – від стадії приблизного розуміння послідовності дій до детального опису кроків і до побудови блок-схеми. Послідовність реалізації кроків плейбуку, наведених в даному розділі, може бути використана практично в незмінному вигляді в будь-якому рішенні класу SOAR.

Так як все одно необхідно зважати на функціональні особливості кожного окремого рішення SOAR, в роботі не наведено приклад реалізації плейбуку в системі для демонстрації універсальності наведеного принципу розробки сценаріїв.

Необхідно також враховувати що кожен крок плейбуку має бути відповідно налаштований в рішенні SOAR, а також необхідне попереднє налаштування інтеграцій з усіма використовуваними рішеннями інформаційної безпеки. Виконання даних налаштувань також потребує доволі високої кваліфікації відповідального співробітника і комунікації різних функціональних груп організації.

ВИСНОВКИ

Отже, в ході виконання кваліфікаційної роботи було досягнуто поставленої мети – розроблено сценарії реагування на інциденти інформаційної безпеки організації для двох типів інцидентів.

1. В ході дослідження теоретичних аспектів побудови ефективного процесу реагування на інциденти інформаційної безпеки було виявлено що організаційні аспекти побудови процесу реагування достатньо освітлені в загальнодоступних джерелах і міжнародних стандартах. Проте опис процесу побудови автоматизованих сценаріїв реагування, що є обов’язковим для впровадження системи реагування на інциденти в великих організаціях, не описаний або описаний недостатньо чи некоректно.

2. Після вивчення доступної теоретичної інформації та стандартів у сфері реагування на інциденти інформаційної безпеки в роботі запропоновано і детально описано принцип розробки автоматизованих сценаріїв реагування.

3. Для подальшої демонстрації використання наведеного плану описано типовий набір рішень інформаційної безпеки великої організації, що можуть бути використані для автоматизації сценарію реагування.

4. В результаті розроблено сценарії реагування на інциденти типу «Фішинг» і «Зловмисне програмне забезпечення», що є одними з найбільш розповсюджених і часто мають бути першочергово впроваджені в організації.

Розроблені сценарії і наведений принцип побудови плейбуків для систематизації і автоматизації реагування на інциденти можуть бути використані будь-якою організацією, що має на меті побудову ефективного процесу реагування на інциденти інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Саврук М.В. Проблеми забезпечення інформаційної безпеки України. Тези доповідей III міжнародної НПК «Інформаційна та економічна безпека». С. 154-155. URL: https://core.ac.uk/download/232881418.pdf

2. Е. І. Низенко, В. П. Каленяк. Забезпечення інформаційної безпеки підприємництва. URL: https://maup.com.ua/assets/files/lib/book/p09_27.pdf

3. Розслідування інцидентів інформаційної безпеки. URL: https://ela.kpi.ua/bitstream/123456789/9600/1/11.pdf

4. Модель побудови системи інформаційної безпеки. URL: https://pidru4niki.com/1237070651274/ekonomika/model_pobudovi_sistemi_informatsiynoyi_bezpeki

5. 10 Common cyber incident response mistakes. URL: https://assets.kpmg/content/dam/kpmg/pdf/2016/04/cyber-incident-response.pdf

6. Top 5 Challenges In Cyber Security Incident Management. URL: https://blog.rsisecurity.com/top-5-challenges-in-cyber-incident-response-management/

7. What is Security Incident Management? The Cybersecurity Incident Management Process, Examples, Best Practices, and More. URL: https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process

8. Система управління інцидентами інформаційної безпеки. URL: https://coggle.it/diagram/XhvYtiTykLSs5M3q/t/%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F-%D1%96%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B0%D0%BC%D0%B8-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1

%96%D0%B9%D0%BD%D0%BE%D1%97-
%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8

9. Миронюк В. Цілі та задачі управління інцидентами інформаційної безпеки. URL:
http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/27130/7460.pdf?sequence=3&isAllowed=y

10. Корченко О., Гнатюк С., Казмірчук С.,Панченко В., Мельник С. Аудит та управління інцидентами інформаційної безпеки. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

11. Юрченко Ю. Рецепт приготування СУІБ в домашніх умовах. URL:
https://www.linkedin.com/pulse/%D1%80%D0%B5%D1%86%D0%B5%D0%BF%D1%82-
%D0%BF%D1%80%D0%B8%D0%B3%D0%BE%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D1%81%D1%83%D1%96%D0%B1-
%D0%B2-
%D0%B4%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D1%96%D1%85-
%D1%83%D0%BC%D0%BE%D0%B2%D0%B0%D1%85-yurii-yurchenko-1

12. CSIRTs by Country - Interactive Map. URL:
https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Ukraine

13. ISO/IEC 27035-3:2020. URL: https://www.iso.org/standard/74033.html

14. ISO/IEC 27035-3. URL: https://kupdf.net/queue/iso-iec-27035-3_59700291dc0d60b33ca88e7e_pdf?queue_id=-1&x=1639242418&z=MTg4LjIzOS44MS42NA

15. NIST Special Publication 800-61. URL:
https://drive.google.com/file/d/1VPtkSsoBoxGY16BtAIt1ExL0snNnEUjy/edit

16. Cyber Security Solutions. URL:
https://www.imperva.com/learn/application-security/cyber-security-solutions/

17. What is Incident Response? Process, Frameworks, and Tools. URL: https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools

18. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1

19. MITRE ATT&CK. URL: https://attack.mitre.org/

20. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

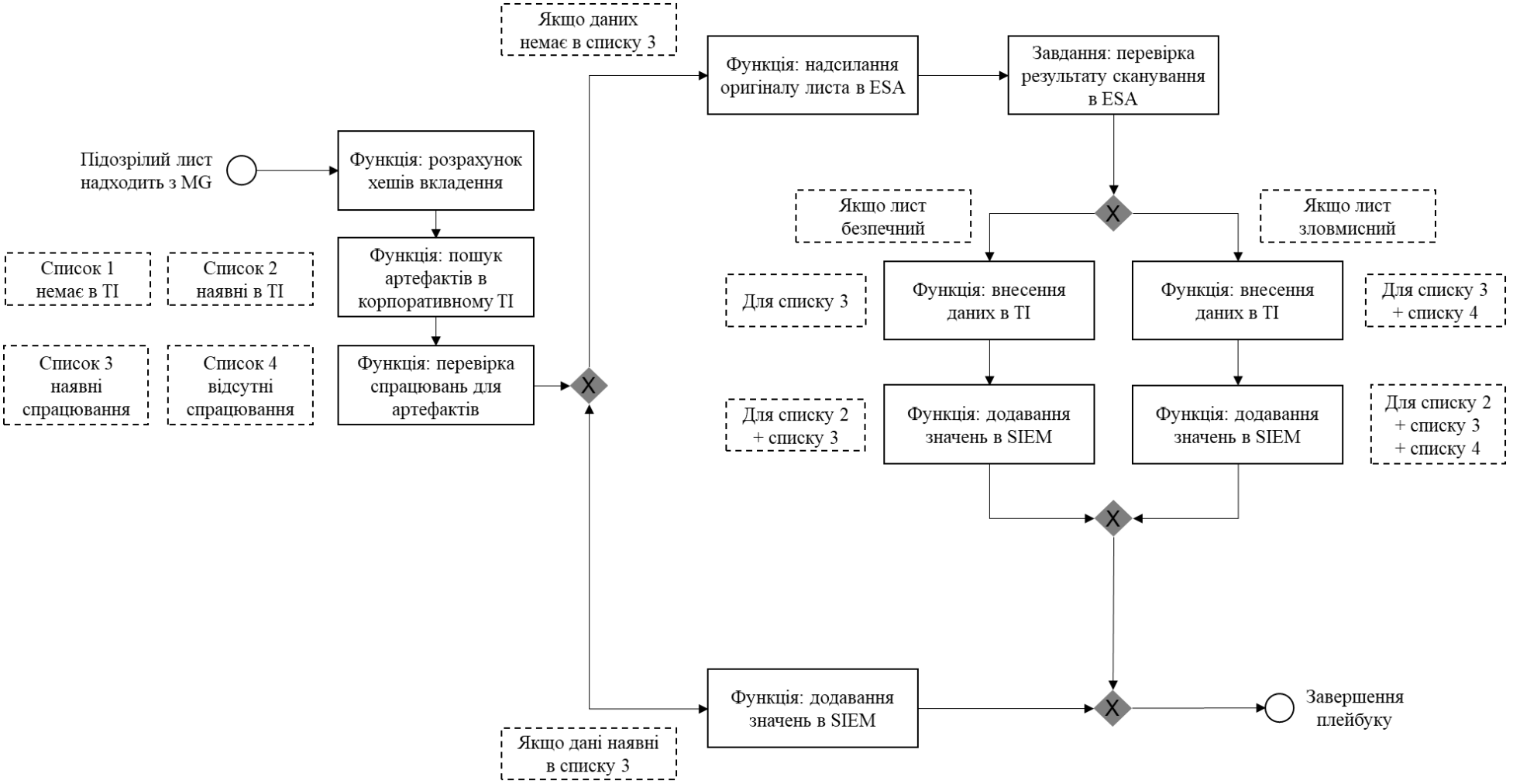

Рис. А.1. Блок-схема сценарію реагування на інцидент типу «Фішинг» (розробка автора)

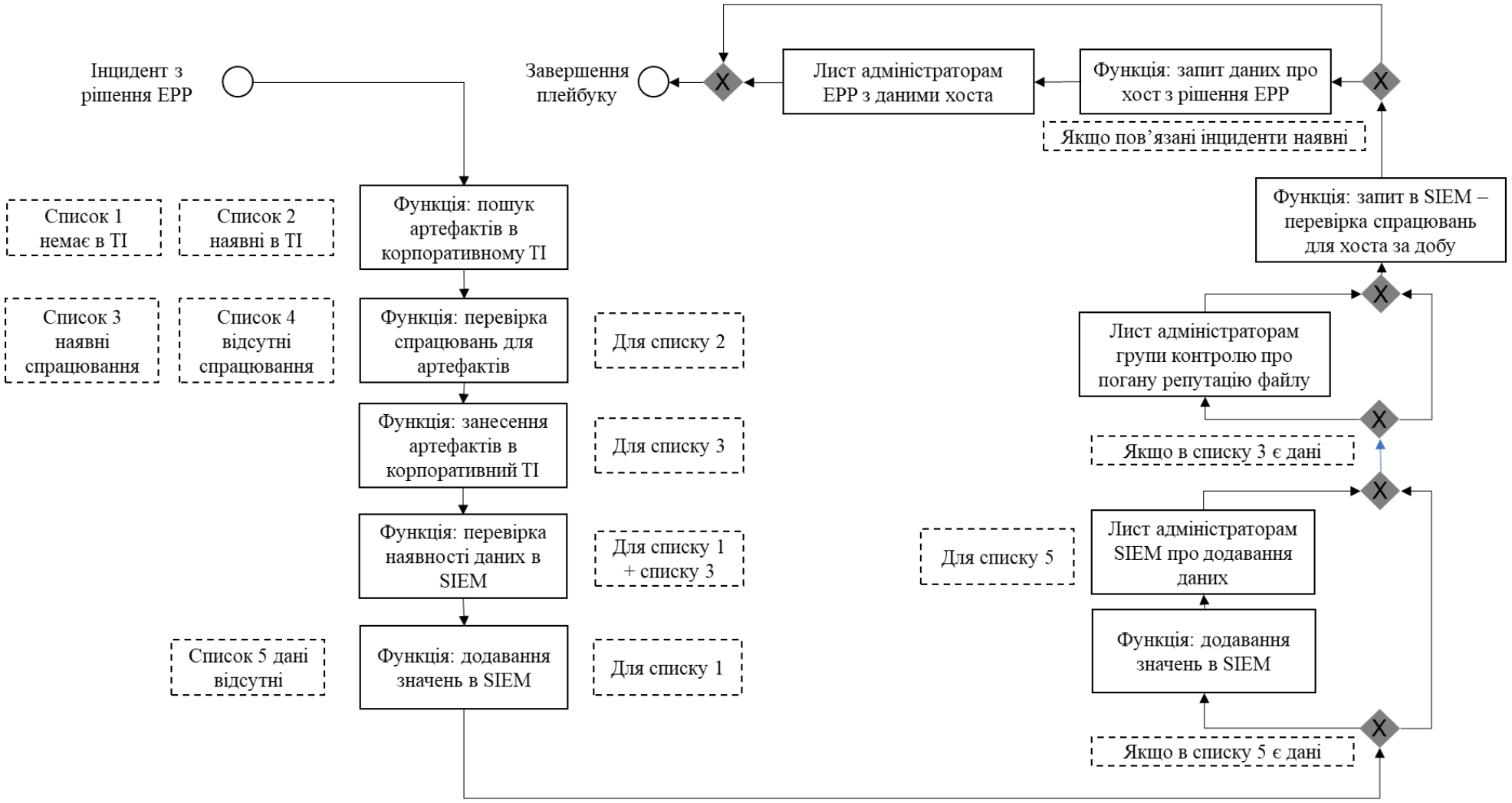

Рис. А.2. Блок-схема сценарію реагування на інцидент типу «Зловмисне програмне забезпечення» (розробка автора)